

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-123032

(P2003-123032A)

(43) 公開日 平成15年4月25日 (2003.4.25)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 K 17/00		G 0 6 K 17/00	T 5 B 0 3 5
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 G 5 B 0 5 8
17/60	4 1 4	17/60	4 1 4 5 B 0 8 5
	5 1 0		5 1 0 5 J 1 0 4
G 0 6 K 19/10		G 0 6 K 19/00	R

審査請求 未請求 請求項の数13 O L (全 19 頁) 最終頁に続く

(21) 出願番号 特願2001-315421(P2001-315421)

(22) 出願日 平成13年10月12日 (2001.10.12)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 相川 慎

神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所デジタルメディア開発本部内

(74) 代理人 110000062

特許業務法人第一国際特許事務所

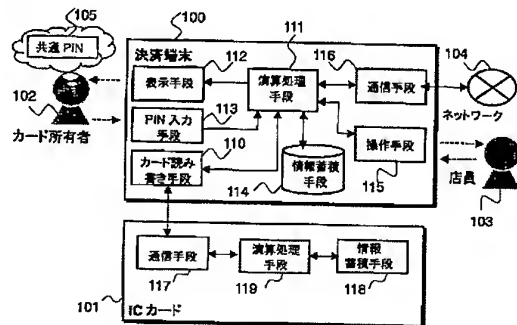
最終頁に続く

(54) 【発明の名称】 ICカード端末および本人認証方法

(57) 【要約】

【課題】 個別PIN認証を必要とする複数のサービスに対応したICカードを用いるサービスにおいて、共通のPINを用いて各サービスを享受できるようにする。

【解決手段】 カード所有者102の正当性確認が必要なサービス処理するサービスプログラムが1個以上とカード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と前記個別暗証番号を暗号化した暗号化暗証番号が1個以上記憶されたICカード101を用いるICカード端末100が、第1の暗証番号を入力する暗証番号入力手段113と、ICカードと通信を行うカード読み書き手段110と、ICカードから読み出した暗号化暗証番号を第1の暗証番号で復号化して第2の暗証番号を生成し、第2の暗証番号をICカードに送信して、ICカード内部で第2の暗証番号が個別暗証番号と一致した場合に、サービスを正常実行する演算処理手段111とを備えた。



【特許請求の範囲】

【請求項1】 カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が1個以上記憶されたICカードを用いるICカード端末であって、前記カード所有者が第1の暗証番号の入力を行える暗証番号入力手段と、前記ICカードと通信を行うカード読み書き手段と、前記暗号化暗証番号を前記カード読み書き手段により前記ICカードから読み出して、前記第1の暗証番号で復号化して、第2の暗証番号を生成し、生成した第2の暗証番号を前記カード読み書き手段により前記ICカードに送信する演算処理手段とを備え、前記ICカード内部で前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行することを特徴とするICカード端末。

【請求項2】 前記ICカードから取得した情報を蓄積しておく情報蓄積手段を設け、前記暗号化暗証番号を前記カード読み書き手段により前記ICカードから読み出して、該情報蓄積手段に蓄積し、該情報蓄積手段に蓄積した前記暗号化暗証番号を読み出して、第1の暗証番号で復号することを特徴とする請求項1に記載のICカード端末。

【請求項3】 前記暗号化暗証番号は、前記個別暗証番号と、特定の値からなる固定値データとを結合したものを、前記第1の暗証番号を用いて暗号化したものであり、前記演算処理手段は、前記暗号化暗証番号を、前記第1の暗証番号を用いて復号化したデータに、前記固定値データが正しく含まれていれば、前記復号化して得られる前記第2の暗証番号は、前記個別暗証番号と等しいと判断することを特徴とする請求項1または請求項2に記載のICカード端末。

【請求項4】 カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号を暗号化した暗号化暗証番号が1個以上記憶されたICカードを用い、前記個別暗証番号を保管しているセンタ装置と通信するICカード端末であって、前記カード所有者が第1の暗証番号の入力を行える暗証番号入力手段と、前記ICカードと通信を行うカード読み書き手段と、ネットワークを介して前記センタ装置と通信する通信手段と、前記カード読み書き手段により前記ICカードから読み出した前記暗号化暗証番号を、前記第1の暗証番号で復号化して、第2の暗証番号を生成し、前記第2の暗証番号を前記通信手段により前記センタ装置に送信する演算処理手段とを備え、前記センタ装置で前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行することを特徴とするICカード端末。

【請求項5】 前記ICカードから取得した情報を蓄積

しておく情報蓄積手段を設け、前記暗号化暗証番号を前記カード読み書き手段により前記ICカードから読み出して、該情報蓄積手段に蓄積し、該情報蓄積手段に蓄積した前記暗号化暗証番号を読み出して、第1の暗証番号で復号することを特徴とする請求項4に記載のICカード端末。

【請求項6】 前記暗号化暗証番号は、前記個別暗証番号と、特定の値からなる固定値データとを結合したものを、前記第1の暗証番号を用いて暗号化したものであり、前記演算処理手段は、前記暗号化暗証番号を、前記第1の暗証番号を用いて復号化したデータに、前記固定値データが正しく含まれていれば、前記復号化して得られる前記第2の暗証番号は、前記個別暗証番号と等しいと判断することを特徴とする請求項5記載のICカード端末。

【請求項7】 カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が1個以上記憶されたICカードと、前記ICカードを用いて前記サービスを前記カード所有者に提供するICカード端末とからなるシステムにおける本人認証方法であって、前記ICカード端末が、前記暗号化暗証番号を前記ICカードから読み出す処理ステップと、前記ICカード端末が前記ICカードから読み出した前記暗号化暗証番号を蓄積する処理ステップと、前記カード保持者が前記ICカード端末に第1の暗証番号を入力する処理ステップと、前記ICカード端末が蓄積している前記暗号化暗証番号を前記第1の暗証番号で復号化して第2の暗証番号を生成する処理ステップと、前記ICカード端末が前記第2の暗証番号を前記ICカードに送信して、前記ICカード内部で前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する処理ステップとを含むことを特徴とする本人認証方法。

【請求項8】 カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号を暗号化した暗号化暗証番号が1個以上記憶されたICカードと、前記ICカードを用いて前記サービスを前記カード所有者に提供するICカード端末と、前記ICカード端末とネットワークを介して接続されていて前記個別暗証番号を保管しているセンタ装置とからなるシステムにおける本人認証方法であって、前記ICカード端末が前記暗号化暗証番号を前記ICカードから読み出す処理ステップと、前記ICカード端末が前記ICカードから読み出した前記暗号化暗証番号を蓄積する処理ステップと、前記カード保持者が前記ICカード端末に第1の暗証番号を入力する処理ステップと、前記ICカード端末が蓄積している前記暗号化暗証番号を前記第1の

暗証番号で復号化して第2の暗証番号を生成する処理ステップと、前記ICカード端末が前記第2の暗証番号を前記センタ装置に送信して、前記センタ装置で前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する処理ステップとを含むことを特徴とする本人認証方法。

【請求項9】 カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が1個以上と、前記暗号化暗証番号を管理する暗証番号管理プログラムとが記憶されたICカードと、前記ICカードを用いて前記サービスを前記カード所有者に提供するICカード端末とからなるシステムにおける本人認証方法であって、前記カード所有者が前記ICカード端末に第1の暗証番号を入力する処理ステップと、前記ICカード端末が前記第1の暗証番号を前記ICカードに送信する処理ステップと、前記ICカード内で実行される前記暗証番号管理プログラムが前記暗号化暗証番号を前記第1の暗証番号で復号化して第2の暗証番号を生成して、前記ICカード端末に送信する処理ステップと、前記ICカード端末が前記第2の暗証番号を前記ICカードに送信して、前記ICカード内部で前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する処理ステップとを含むことを特徴とする本人認証方法。

【請求項10】 カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が1個以上と、前記暗号化暗証番号を管理する暗証番号管理プログラムとが記憶されたICカードと、前記ICカードを用いて前記サービスを前記カード所有者に提供するICカード端末とからなるシステムにおける本人認証方法であって、前記カード保持者が前記ICカード端末に第1の暗証番号を入力する処理ステップと、前記ICカード端末が前記第1の暗証番号を前記ICカードに送信する処理ステップと、前記ICカード内で実行される前記暗証番号管理プログラムが前記暗号化暗証番号を前記第1の暗証番号で復号化して第2の暗証番号を生成する処理ステップと、前記暗証番号プログラムが、前記サービスプログラムに第2の暗証番号を送信して、前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する処理ステップとを含むことを特徴とする本人認証方法。

【請求項11】 カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を外部に出力することを保護する第1の暗証番号とが記憶されたICカ

ードを用いて前記サービスを前記カード所有者に提供するICカード端末であって、前記カード所有者が第2の暗証番号の入力を行える暗証番号入力手段と、前記ICカードと通信を行うカード読み書き手段と、前記第2の暗証番号を前記ICカード読み書き手段により前記ICカードに送信して、前記ICカード内部で、前記第2の暗証番号が前記第1の暗証番号と一致した場合に、前記個別暗証番号を前記ICカード読み書き手段により取得し、前記個別暗証番号を前記カード読み書き手段により前記ICカードに送信して、前記ICカード内部での前記個別暗証番号の照合が成功した場合に、前記サービスを正常実行する演算処理手段とを有することを特徴とするICカード端末。

【請求項12】 カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を外部に出力することを保護する第1の生体情報と、生体情報を管理する管理プログラムとが記憶されたICカードを用いて前記サービスを前記カード所有者に提供するICカード端末において、第2の生体情報を前記カード所有者から読み取ることができる生体情報読み取り手段と、前記ICカードと通信を行うカード読み書き手段と、前記第2の生体情報を前記ICカード読み書き手段により前記ICカードに送信して、前記ICカード内部で、前記第2の生体情報が前記第1の生体情報と一致した場合に、前記個別暗証番号を前記ICカード読み書き手段により取得し、前記個別暗証番号を前記カード読み書き手段により前記ICカードに送信して、前記ICカード内部での前記個別暗証番号の照合が成功した場合に、前記サービスを正常実行する演算処理手段とを有することを特徴とするICカード端末。

【請求項13】 前記第1の生体情報および前記第2の生体情報は、指紋を用いることを特徴とする請求項12に記載のICカード端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカードを用いて本人認証を行なうICカード端末装置および本人認証方法に関する。

【0002】

【従来の技術】近年、ICカードが磁気カードに代わって広く普及しつつある。これはICカードには、記憶容量が大きい、暗号処理などを行なうための演算装置（マイクロプロセッサ）を備えている、容易に内部を観察できない（耐タンパ性を有している）といった、磁気カードにはない特徴があるからである。このような特徴を持ったICカードを、決済システムや身分証明システムなどに適用することで、磁気カードに比べてセキュリティを向上させたり、磁気カードでは実現できなかった新し

いサービスを提供したりすることができる。例えば、決済システムが提供するサービスとしては電子マネーやクレジットカードがあり、身分証明システムが提供するサービスとしては社員IDカードや運転免許証などがあげられる。

【0003】ICカードは、その通信方式により、接触型と非接触型に分類されており、それぞれの仕様はすでに標準化されている。例えば、接触型ICカードは、ISO (International Organization for Standardization: 10

国際標準化機構)で、ISO/IEC7816として標準化されている。ISO/IEC7816に基づくICカードは、端末から送信するコマンドに従って内部で演算を行い、結果をレスポンスとして返すということを順次行なっていくことで、サービスを実現するための処理を遂行していく。

【0004】ここで、ICカード間で送受信するコマンドとレスポンスは、APDU (Application Protocol Data Unit) という形式でISO/IEC7816で規定している。また、ISO/IEC7816に基づくICカードは、図13に示すようにプログラムやデータは階層構造を持ったファイルに格納される。

【0005】図13において、主ファイル(MF)900は、最上位層のファイルでありICカード内に一つだけ存在し、その下に複数の専用ファイル(DF)901A、901B、および901Cが存在する。専用ファイルには特定のサービスを実行するためのプログラム(以下サービスプログラムと呼ぶ)とサービス実行に必要なデータ(以下サービスデータと呼ぶ)が格納される。専用ファイルはICカード内に複数存在可能なので、複数のサービスプログラムとサービスデータを、異なる専用ファイルに格納することで、1枚のICカードで複数のサービスを利用できるようになる。

【0006】特定のサービスプログラムを実行するためには、まず端末が、APDU形式のコマンドとして規定されている「ファイル選択コマンド」を用いて、特定のサービスプログラムが格納されている専用ファイルを、カレントのファイルとして選択する。これにより、それ以降にICカードが端末から受信するコマンドは、選択されたサービスプログラムに従って処理されるようになる。ここで、各専用ファイルは、アプリケーション識別子(以下AIDと略す)と呼ばれるIDにより外部から識別可能である。例えば、「ファイル選択コマンド」は、AIDを指定することで、特定の専用ファイルを選択することができる。

【0007】さて、ICカードを用いてサービスを受ける場合、カード所有者本人がそのカードを使用していることの認証を行なうことが求められる場合があり、このために行う認証は本人認証と呼ばれる。本人認証を実現

するための方法としては、PINと呼ばれる暗証番号をカード所有者が端末に入力するPIN認証が一般的である。PIN認証には、カード所有者が入力したPINをICカード内に記憶しているPINと照合する「オフラインPIN認証」と、カード所有者が入力したPINを、ネットワークを介してセンタが保持しているPINと照合する「オンラインPIN認証」とがある。PIN認証などの本人認証を行なうことは、ICカードの不正利用を防止するために重要である。

【0008】

【発明が解決しようとする課題】以上説明したように、ICカードを用いることで、様々なサービスを1枚のICカードで利用できるようになるが、一方で、各サービスを利用するためにPIN認証を行なう場合に、カード所有者はサービス毎に異なるPINを覚えておき、利用するサービス毎にPINを使い分けなければならない可能性がある。これはカード利用者の利便性を大きく損なう要因となる。

【0009】そこで、本発明は、ICカード所有者が、複数のサービスに対応したICカードを用いて各サービスを受ける場合に、サービス毎に行なう必要のあるPIN認証を、共通のPINを一つ覚えておくだけで実行できる構成にすることで、ICカード所有者の利便性を向上できるICカード端末および、本人認証方法を提供することを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するために、本発明では、カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が1個以上記憶されたICカードを用いるICカード端末が、前記カード所有者が第1の暗証番号の入力を行える暗証番号入力手段と、前記ICカードと通信を行うカード読み書き手段と、前記ICカードから取得した情報を蓄積しておく情報蓄積手段と、前記暗号化暗証番号を前記カード読み書き手段により前記ICカードから読み出して、前記情報蓄積手段に蓄積し、前記情報蓄積手段に蓄積した前記暗号化暗証番号を読み出して、前記第1の暗証番号で復号化して、第2の暗証番号を生成し、前記第2の暗証番号を前記カード読み書き手段により前記ICカードに送信して、前記ICカード内部で前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する演算処理手段とを有している。

【0011】また、本発明では、カード所有者の正当性確認が必要なサービスを処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が1個以上記憶されたIC

カードと、前記 IC カードを用いて前記サービスを前記カード所有者に提供する IC カード端末とからなるシステムにおける本人認証方法が、前記 IC カード端末が前記暗号化暗証番号を前記 IC カードから読み出す処理ステップと、前記 IC カード端末が前記 IC カードから読み出した前記暗号化暗証番号を蓄積する処理ステップと、前記カード保持者が前記 IC カード端末に第 1 の暗証番号を入力する処理ステップと、前記 IC カード端末が蓄積している前記暗号化暗証番号を前記第 1 の暗証番号で復号化して第 2 の暗証番号を生成する処理ステップと、前記 IC カード端末が前記第 2 の暗証番号を前記 IC カードに送信して、前記 IC カード内部で前記第 2 の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する処理ステップとを含んでいる。

【0012】すなわち、上記課題を解決するために、本発明は、カード所有者の正当性確認が必要なサービス进行处理するサービスプログラムが 1 個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が 1 個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が 1 個以上記憶された IC カードを用いる IC カード端末が、前記カード所有者が第 1 の暗証番号の入力を行える暗証番号入力手段と、前記 IC カードと通信を行うカード読み書き手段と、前記暗号化暗証番号を前記カード読み書き手段により前記 IC カードから読み出して、前記第 1 の暗証番号で復号化して、第 2 の暗証番号を生成し、生成した第 2 の暗証番号を前記カード読み書き手段により前記 IC カードに送信する演算処理手段とを備え、前記 IC カード内部で前記第 2 の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行するようにした。

【0013】本発明は、上記 IC カード端末において、前記 IC カードから取得した情報を蓄積しておく情報蓄積手段を設け、前記暗号化暗証番号を前記カード読み書き手段により前記 IC カードから読み出して、該情報蓄積手段に蓄積し、該情報蓄積手段に蓄積した前記暗号化暗証番号を読み出して、第 1 の暗証番号で復号するようにした。

【0014】本発明は、上記 IC カード端末において、前記暗号化暗証番号は、前記個別暗証番号と、特定の値からなる固定値データとを結合したものを、前記第 1 の暗証番号を用いて暗号化したものであり、前記演算処理手段は、前記暗号化暗証番号を、前記第 1 の暗証番号を用いて復号化したデータに、前記固定値データが正しく含まれていれば、前記復号化して得られる前記第 2 の暗証番号は、前記個別暗証番号と等しいと判断することとした。

【0015】上記課題を解決するために、本発明は、カード所有者の正当性確認が必要なサービス进行处理するサービスプログラムが 1 個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号を暗号化した

暗号化暗証番号が 1 個以上記憶された IC カードを用い、前記個別暗証番号を保管しているセンタ装置と通信する IC カード端末が、前記カード所有者が第 1 の暗証番号の入力を行える暗証番号入力手段と、前記 IC カードと通信を行うカード読み書き手段と、ネットワークを介して前記センタ装置と通信する通信手段と、前記カード読み書き手段により前記 IC カードから読み出した前記暗号化暗証番号を、前記第 1 の暗証番号で復号化して、第 2 の暗証番号を生成し、前記第 2 の暗証番号を前記通信手段により前記センタ装置に送信する演算処理手段とを備え、前記センタ装置で前記第 2 の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行することとした。

【0016】本発明は、上記 IC カード端末において、前記 IC カードから取得した情報を蓄積しておく情報蓄積手段を設け、前記暗号化暗証番号を前記カード読み書き手段により前記 IC カードから読み出して、該情報蓄積手段に蓄積し、該情報蓄積手段に蓄積した前記暗号化暗証番号を読み出して、第 1 の暗証番号で復号するようにした。

【0017】本発明は、上記 IC カード端末において、前記暗号化暗証番号は、前記個別暗証番号と、特定の値からなる固定値データとを結合したものを、前記第 1 の暗証番号を用いて暗号化したものであり、前記演算処理手段は、前記暗号化暗証番号を、前記第 1 の暗証番号を用いて復号化したデータに、前記固定値データが正しく含まれていれば、前記復号化して得られる前記第 2 の暗証番号は、前記個別暗証番号と等しいと判断することとした。

【0018】上記課題を解決するために、本発明は、カード所有者の正当性確認が必要なサービス进行处理するサービスプログラムが 1 個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が 1 個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が 1 個以上記憶された IC カードと、前記 IC カードを用いて前記サービスを前記カード所有者に提供する IC カード端末とからなるシステムにおける本人認証方法が、前記 IC カード端末が、前記暗号化暗証番号を前記 IC カードから読み出す処理ステップと、前記 IC カード端末が前記 IC カードから読み出した前記暗号化暗証番号を蓄積する処理ステップと、前記カード保持者が前記 IC カード端末に第 1 の暗証番号を入力する処理ステップと、前記 IC カード端末が蓄積している前記暗号化暗証番号を前記第 1 の暗証番号で復号化して第 2 の暗証番号を生成する処理ステップと、前記 IC カード端末が前記第 2 の暗証番号を前記 IC カードに送信して、前記 IC カード内部で前記第 2 の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する処理ステップとを含むようにした。

【0019】上記課題を解決するために、本発明は、カ

ード所有者の正当性確認が必要なサービス処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号を暗号化した暗号化暗証番号が1個以上記憶されたICカードと、前記ICカードを用いて前記サービスを前記カード所有者に提供するICカード端末と、前記ICカード端末とネットワークを介して接続されていて前記個別暗証番号を保管しているセンタ装置とからなるシステムにおける本人認証方法が、前記ICカード端末が前記暗号化暗証番号を前記ICカードから読み出す処理ステップと、前記ICカード端末が前記ICカードから読み出した前記暗号化暗証番号を蓄積する処理ステップと、前記カード保持者が前記ICカード端末に第1の暗証番号を入力する処理ステップと、前記ICカード端末が蓄積している前記暗号化暗証番号を前記第1の暗証番号で復号化して第2の暗証番号を生成する処理ステップと、前記ICカード端末が前記第2の暗証番号を前記センタ装置に送信して、前記センタ装置で前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する処理ステップとを含むようにした。

【0020】上記課題を解決するために、本発明は、カード所有者の正当性確認が必要なサービス処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が1個以上と、前記暗号化暗証番号を管理する暗証番号管理プログラムとが記憶されたICカードと、前記ICカードを用いて前記サービスを前記カード所有者に提供するICカード端末とからなるシステムにおける本人認証方法が、前記カード所有者が前記ICカード端末に第1の暗証番号を入力する処理ステップと、前記ICカード端末が前記第1の暗証番号を前記ICカードに送信する処理ステップと、前記ICカード内で実行される前記暗証番号管理プログラムが前記暗号化暗証番号を前記第1の暗証番号で復号化して第2の暗証番号を生成して、前記ICカード端末に送信する処理ステップと、前記ICカード端末が前記第2の暗証番号を前記ICカードに送信して、前記ICカード内部で前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する処理ステップとを含むようにした。

【0021】上記課題を解決するために、本発明は、カード所有者の正当性確認が必要なサービス処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を暗号化した暗号化暗証番号が1個以上と、前記暗号化暗証番号を管理する暗証番号管理プログラムとが記憶されたICカードと、前記ICカードを用いて前記サービスを前記カード所有者に提供するICカード端末とからなるシステムにおける本人認証方法が、前記カード保持者が前記ICカード端末に第1の

暗証番号を入力する処理ステップと、前記ICカード端末が前記第1の暗証番号を前記ICカードに送信する処理ステップと、前記ICカード内で実行される前記暗証番号管理プログラムが前記暗号化暗証番号を前記第1の暗証番号で復号化して第2の暗証番号を生成する処理ステップと、前記暗証番号プログラムが、前記サービスプログラムに第2の暗証番号を送信して、前記第2の暗証番号が前記個別暗証番号と一致した場合に、前記サービスを正常実行する処理ステップとを含むようにした。

【0022】上記課題を解決するために、本発明は、カード所有者の正当性確認が必要なサービス処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を外部に出力することを保護する第1の暗証番号とが記憶されたICカードを用いて前記サービスを前記カード所有者に提供するICカード端末が、前記カード所有者が第2の暗証番号の入力を行える暗証番号入力手段と、前記ICカードと通信を行うカード読み書き手段と、前記第2の暗証番号を前記ICカード読み書き手段により前記ICカードに送信して、前記ICカード内部で、前記第2の暗証番号が前記第1の暗証番号と一致した場合に、前記個別暗証番号を前記ICカード読み書き手段により取得し、前記個別暗証番号を前記カード読み書き手段により前記ICカードに送信して、前記ICカード内部での前記個別暗証番号の照合が成功した場合に、前記サービスを正常実行する演算処理手段とを備えた。

【0023】上記課題を解決するために、本発明は、カード所有者の正当性確認が必要なサービス処理するサービスプログラムが1個以上と、前記カード所有者の正当性確認を行うために用いる個別暗証番号が1個以上と、前記個別暗証番号を外部に出力することを保護する第1の生体情報と、生体情報を管理する管理プログラムとが記憶されたICカードを用いて前記サービスを前記カード所有者に提供するICカード端末が、第2の生体情報を前記カード所有者から読み取ることができる生体情報読み取り手段と、前記ICカードと通信を行うカード読み書き手段と、前記第2の生体情報を前記ICカード読み書き手段により前記ICカードに送信して、前記ICカード内部で、前記第2の生体情報が前記第1の生体情報と一致した場合に、前記個別暗証番号を前記ICカード読み書き手段により取得し、前記個別暗証番号を前記カード読み書き手段により前記ICカードに送信して、前記ICカード内部での前記個別暗証番号の照合が成功した場合に、前記サービスを正常実行する演算処理手段とを備えた。

【0024】本発明は、上記ICカード端末において、前記第1の生体情報および前記第2の生体情報として、指紋を用いた。

【0025】

【発明の実施の形態】以下、本発明の実施形態について説明していく。ここで、以下の実施形態では、接触型のICカードを用いた場合について説明していくが、接触型であることは本発明に必要な項目では無く、例えば非接触ICカードであっても本発明は適用可能である。また、以下の実施形態では、端末とICカードとの間で送受信するコマンドは、APDU形式のコマンドを想定しているが、APDU形式のコマンドを用いることは本発明に必要な項目では無く、APDU形式と同等の機能を実現できるコマンドセットであれば、どのようなものを用いても本発明は適用可能である。さらに、以下の実施形態では、端末として電子マネーやクレジットカードのための決済を行なう機能を有した端末を想定しているが、このような端末であることは本発明に必要な項目ではなく、本人認証を行なう端末であれば本発明は適用可能である。

【0026】まず、第1の実施形態について説明する。図1に、本人認証を行う本実施形態に係わるICカードおよび端末の構成を示す。図1において、本人認証は、決済端末100と、ICカード101と、カード所有者102と、店員103と、ネットワーク104との間で行われる。図1に示した構成は、カード所有者102が、ICカード101を用いて、電子マネーやクレジットカードによる決済を行なうことを想定している。したがって、決済端末100は、ICカードによる決済機能を備えた端末であり、例えばクレジットカードや金融機関のATMを想定している。また、ICカード101は、電子マネーやクレジットカード等の複数のサービスを提供できる構成となっている。カード所有者102は、本人認証のために使用するPINであってICカード101が提供する複数のサービスで共通に使用できる共通PIN105を、記憶しているものとする。

【0027】次に、決済端末100の内部構成について説明する。決済端末100は、カード読み書き手段110、演算処理手段111、表示装置112、PIN入力手段113、情報蓄積手段114、操作手段115、通信手段116を有する。

【0028】カード読み書き手段110は、ICカード101と通信するために、ICカード101にコマンドを送信（書込み）したり、ICカードからレスポンスを受信（読み込み）したりする機能を有する。

【0029】演算処理手段111は、例えばマイクロプロセッサとプログラム格納メモリから成り、プログラム格納メモリに格納されているプログラムに基づいて、決済端末100全体を制御し、決済処理を遂行する機能を有する。

【0030】表示手段112は、カード所有者102に対して、例えば決済金額等の各種情報を表示する。

【0031】PIN入力手段113は、カード所有者102が本人認証のためのPINを、例えばテンキー等を

用いて入力できる機能を有する。

【0032】情報蓄積手段114は、ICカード101やネットワーク104から取得した情報、あるいは、カード所有者102や店員103が入力した情報を一時的あるいは永続的に蓄積する機能を有し、例えばハードディスクや半導体メモリ等から構成される。

【0033】操作手段115は、店員103が決済端末100を操作するためのインターフェイスを提供し、例えば、キーボード、バーコードリーダー、ディスプレイ等から構成される。

【0034】通信手段116は、ネットワーク104を介してセンタと通信する機能を有し、例えばオンラインPIN認証を行なうために使用する。ここで、決済端末100が金融機関ATM等の無人端末の場合は、操作手段115は無くてもよく、店員103も存在しなくてよい。また、決済端末100による決済処理がオフラインで完了するような場合は、通信手段116は無くてもよい。

【0035】次に、ICカード101の内部構成について説明する。ICカード101は、通信手段117、情報蓄積手段118、演算処理手段119を有する。

【0036】通信手段117は、決済端末100のカード読み書き手段110と通信を行ない、決済端末100からコマンドを受信したり、決済端末100にレスポンスを返信したりする機能を有する。

【0037】情報蓄積手段118は、ICカードが提供するサービスを実行するプログラムやデータ、あるいは決済端末100から取得した情報等を一時的あるいは永続的に格納する機能を有し、例えば、ROM (Read Only Memory)、RAM (Random Access Memory)、フラッシュメモリ等の半導体メモリから構成される。

【0038】演算処理手段119は、マイクロプロセッサを用いることで、ICカード全体の制御を司り、情報蓄積手段118に格納されているプログラムを実行する機能を有する。

【0039】次に、本実施形態に係わるICカード101に格納される情報の構成を図2に示す。図2は、ICカード101を構成する情報蓄積手段118内部のファイル構成であり、主ファイル(MF)120、専用ファイル(DF)121A、121B、121C、およびPIN管理専用ファイル122から構成される。これらのファイルは階層構造となっており、主ファイル120が最上位に位置し、その下位層に、専用ファイル121A、121B、121C、およびPIN管理専用ファイル122が位置する構成となっている。それぞれの専用ファイルには異なるAIDが割り当てられており、外部から識別可能である。

【0040】次に、専用ファイル121A、121Bおよび121Cの内部構成について説明する。専用ファイ

10

20

30

40

50

ル121Aには、特定の決済サービスを実行するサービスプログラム131Aと、この決済サービスにおいて本人認証をオフラインPIN認証により実行するために必要なデータである、個別PIN141Aが格納されている。同様に専用ファイル121Bには、サービスプログラム131Bと、個別PIN141Bが格納されている。また、専用ファイル121Cには、サービスプログラム131Cが格納されていて、サービスプログラム131Cにより実行される決済サービスは、本人認証として、オンラインPIN認証を行なうものとする。したがって、専用ファイル121C内には、PINデータは格納されていない。

【0041】次に、PIN管理専用ファイル122について説明する。PIN管理専用ファイル122は、PIN管理用の専用ファイルである。PIN管理専用ファイル122には、サービスプログラム131A、131B、および131Cで個別に使用する個別PINを管理するPIN管理プログラム132と、PIN管理プログラム132が管理するデータである、PIN管理データ142A、142B、および142Cとが格納されている。ここでPIN管理データ142Aは、サービスプログラム131Aにより実行されるオフラインPIN認証に必要なデータが含まれている。同様に、PIN管理データ142Bは、サービスプログラム131Bにより実行されるオフラインPIN認証に必要なデータが含まれている。また、PIN管理データ142Cは、サービスプログラム131Cにより実行されるオンラインPIN認証に必要なデータが含まれている。

【0042】この説明では、情報蓄積手段118には、3つのサービスプログラムが含まれていて、PIN管理プログラムは3つのPIN管理データを管理している構成になっているが、任意の数のサービスプログラムが含まれているICカードにも本発明は適用可能である。例えば、ICカード101が4個のサービスプログラムを含む場合は、PIN管理プログラムは、4個のPIN管理データを管理すればよい。さらに、本発明は、ICカード101内のサービスプログラムがオンラインPIN認証を行なう構成であっても、オフラインPIN認証を行なう構成であっても適用することができる。

【0043】次に、本実施形態に係わるPIN管理プログラム132が管理しているPIN管理データの構成と使用方法について説明していく。まず、PIN管理データの構成と生成手順を図3に示す。図3において、PIN管理データ142は、AID202と、制御フラグ203と、暗号化個別PIN204が含まれる構成となっている。AID202は、PIN管理データ142が対応しているサービスプログラムが格納されている専用ファイルのアプリケーション識別子である。制御フラグ203はPIN管理データ142が対応するPIN認証方式（オンラインあるいはオフライン）を示す。例えば、

制御フラグ203に1ビットを割り当てて、「0」の場合はオンライン用の個別PIN、「1」の場合はオフライン用の個別PINがPIN管理データ142に保持されているものとする。暗号化個別PIN204は、個別PINを暗号化したものであり、暗号化個別PIN204だけからでは元の個別PINの内容は推測できない。

【0044】PIN管理データ142の生成手順としては、まず、ステップS200として、正しいAID202を設定する。次にステップS201として、正しい制御フラグ203を設定する。次に、ステップS202として、個別PIN141と固定パターン201を結合したデータを、カード所有者が設定した共通PIN105を暗号鍵として暗号化処理を行い、出力される暗号文を暗号化個別PIN204とする。ここで、固定パターン201はある特定のビット列であり、固定値として定めておく。またステップS202で実行する暗号化処理としては、例えばブロック暗号方式に基づいた暗号アルゴリズムであるDESを用いることが考えられる。あるいは他の暗号化アルゴリズムを用いてもよい。

【0045】以上の生成手順は、新しくPIN管理データ142を登録する時、共通PIN105を変更する時、および個別PIN141を変更する時に行われる。共通PINを変更する場合は、新しい共通PINで生成したPIN管理データを、今までのPIN管理データと置き換えればよい。同様に、個別PINを変更する場合は、新しい個別PINから生成したPIN管理データを、今までのPIN管理データと置き換えればよい。

【0046】次に、PIN管理データから個別PINを抽出する処理手順を図4に示す。この処理手順は、図1に示した決済端末100を構成する演算処理手段111を用いることで実行される。図4において、PIN管理データ142は、前述したように、AID202と、制御フラグ203と、暗号化個別PIN204が含まれる構成となっている。

【0047】まず、ステップS300としてAID202をチェックし、個別PINを使用するサービスプログラムが格納されている専用ファイルのアプリケーション識別子と一致するかを調べる。もし、AIDが一致しなければ本処理を不正終了する。AIDが一致するならば、次にステップS301として、制御フラグ203をチェックし、制御フラグ203が示すPIN認証方式（オフラインあるいはオンライン）と、個別PINを使用するサービスプログラムが行なうPIN認証方式とが一致するかを調べる。もし、PIN認証方式が一致しなければ処理を不正終了する。PIN認証方式が一致する場合は、次にステップS302として、共通PIN105を暗号鍵として、復号化処理を行い、出力される平文を個別PIN141と固定パターン201とに分離する。ここで、共通PIN105としては、カード所有者102が、端末100に入力したものを使用する。

【0048】次に、ステップS303として、取得した固定パターン201が正しい値であるかどうかを検証する。ここで、端末100は固定パターンの正しい値を予め知っているものとする。もし、固定パターン201が正しい値でなければ、本処理を不正終了する。固定パターン201が正しい値であれば、個別PIN141を正しく取得できたと見なし、本処理を正常終了する。

【0049】次に、本実施形態に係わる決済端末100の処理フローを説明していく。図5は、カード所有者102が、ICカード101を用いて、決済端末100で決済処理を行なうときのフロー図である。ここで、この決済処理は、図1で示した決済端末100を構成する演算処理手段111を用いて実行するものとする。また、この例では、ICカードは、サービスプログラム131と、PIN管理プログラム132を格納しているが、決済端末100はICカード101内に格納されている複数のプログラムと同時に通信を行わないものとする。また、決済端末100がICカード101に送信するコマンドはAPDU形式を用いるものとして説明していく。

【0050】まず、ICカード101が決済端末100に挿入されると、ステップS500としてICカードの初期化処理を行なう。この処理では、決済端末100がICカード101にリセット要求を送信し、その後ICカード101からリセット応答を受信するといったことが行なわれる。次に、決済端末100は、ステップS501としてICカード101に格納されている全てのPIN管理データを読み出す。この処理では、まず決済端末100が、ファイル選択コマンドをICカード101に発行することで、PIN管理プログラム132が格納されているPIN管理専用ファイルを選択する。つづいて、決済端末100がデータ読出しコマンドをPIN管理プログラム132に発行することで、PIN管理データ142を全て読み出す。読み出されたPIN管理データは、図1に示した情報蓄積手段114に格納しておく。

【0051】次に、ステップS502として、端末100は、カード所有者102の選択等により、ICカード101内に格納されているサービスプログラム131を選択する。この処理では、まず決済端末100が、ファイル選択コマンドをICカード101に発行することで、サービスプログラム131が格納されている専用ファイルを選択する。つづいて、決済端末100が特定のコマンドをサービスプログラム131に発行していくことで、サービスプログラム131に基づいた処理を、PIN認証が必要になるまで行なっていく。

【0052】次に、カード所有者102が共通PIN105を入力すると、ステップS503として、端末100に入力された共通PINを用いて、先にICカードから読み出したPIN管理データから個別PINを復号す

る。この処理では、ICカードから読み出した全てのPIN管理データに対して、図4を用いて説明した個別PINを抽出する処理を成功するまで実行する。ここで、もし個別PINの抽出処理が失敗に終わったら、決済処理を中断するという運用方法がまず考えられる。あるいは、個別PINの抽出処理が失敗したら、端末100に入力された共通PINを個別PINとみなして以降の決済処理を継続するという運用方法も考えられる。後者の場合については、ステップS503としてカード所有者102は、共通PINあるいは個別PINのいずれかを入力してよい場合の運用方法になる。

【0053】次に、ステップS504として、PIN認証をオフラインで行なうかオンラインで行なうかをチェックする。もしオフラインPIN認証を行なうなら、ステップS505として、決済端末100は抽出した個別PINをICカード101に送信する。この処理では、決済端末100はPIN検証コマンドをサービスプログラム131に発行することで、ICカード101に個別PINを送信し、内部で個別PINの照合を行なわせる。一方でもしオンライン認証を行なうのなら、ステップS506として、決済端末100は抽出した個別PINを、ネットワークを介してセンタに送信する。以上説明した手順に従って、オフラインPIN認証あるいはオンラインPIN認証が終了した後、ステップS507として、端末100は残りの決済処理を、ICカード101に特定のコマンド発行するなどして継続していく。

【0054】次に、第2の実施形態について説明する。本実施形態に係わるICカードおよび決済端末の構成は、第1の実施形態で図1を用いて説明で示した構成と同様である。また、本実施形態に係わるICカードに格納される情報の構成は、第1の実施形態で図2を用いて説明した構成と同様である。さらに、PIN管理データから個別PINを抽出する処理手順は、第1の実施形態で図4を用いて説明した処理手順と同様である。ただし本実施形態では、端末100は、ICカード101に格納されているPIN管理プログラム、および複数のサービスプログラムと、同時に通信することが可能であるものとする。また、本実施形態では、ICカード101に格納されているPIN管理プログラム132が、PIN管理データから個別PINを抽出する処理を行なうものとする。

【0055】以下、本実施形態の実現方法について示す。まず、図6は、APDU形式のコマンドの構成図である。図6において、APUD形式のコマンドは、クラス610、命令611、パラメータ1(612)、パラメータ2(613)、Lc614、データ615、およびLe616から構成される。クラス610は、コマンドを用いて通信するサービスプログラムの識別子である。命令611は、コマンドの命令コードを示す。パラメータ1(612)とパラメータ2(613)は、命令

10

20

30

40

50

611に依存したパラメータの値を格納する。Lc614は、次のフィールドであるデータ615の長さを表す。データ615はICカードに送信するデータを格納するフィールドである。Le616はICカードから送り返されるレスポンスの長さを表す。

【0056】さらに、図6において、クラス610は、命令タイプ620、セキュリティメッセージタイプ621、および論理チャンネル番号622から構成される。命令タイプ620は、命令611を分類するためのフィールドである。セキュリティメッセージタイプは、データ615の盗聴や改ざんを防止するための暗号化処理を行なうかどうかを表すフィールドである。論理チャンネル番号622は、ICカードに格納されているプログラムに発行するコマンドを論理的なアドレスを用いて区別するために用いる。すなわち、論理チャンネル番号622の値を異ならせることで、ICカード内の複数のプログラムと、同時に通信することが可能になる。

【0057】以上の説明では、APDU形式のコマンドを例にとって説明したが、論理チャンネルを用いた機能と同等の機能を有していれば、他の形式のコマンドであっても、本発明に適用可能である。

【0058】次に、本実施形態に係わる決済端末100の処理フローを説明していく。図7は、カード所有者102が、ICカード101を用いて、決済端末100で決済処理を行なうときのフロー図である。この例では、決済端末100がICカード101に送信するコマンドはAPDU形式を用いるものとして説明していく。また、ICカードは、サービスプログラム131とPIN管理プログラム132を格納しており、決済端末100は、サービスプログラム131に発行するコマンドの論理チャンネル番号として、論理チャンネルAを用い、PIN管理プログラム132に発行するコマンドの論理チャンネル番号として、論理チャンネルBを用いて、同時に通信を行なうものとする。

【0059】まず、ICカード101が決済端末100に挿入されると、ステップS700としてICカードの初期化処理を行なう。この処理では、決済端末100がICカード101にリセット要求を送信し、その後ICカード101からリセット応答を受信するといったことが行なわれる。

【0060】次に、決済端末100は、ステップS701として、カード所有者102の選択等により、ICカード101内に格納されているサービスプログラム131を選択する。この処理では、まず決済端末100が、ファイル選択コマンドを、論理チャンネルAを用いてICカード101に発行することで、サービスプログラム131が格納されている専用ファイルを選択する。つづいて、決済端末100が特定のコマンドを論理チャンネルAを用いてサービスプログラム131に発行していくことで、サービスプログラム131に基づいた処理を、

PIN認証が必要になるまで行なっていく。

【0061】ここで、PIN認証を実行する前に、決済端末100は、ステップS702として、ファイル選択コマンドを論理チャンネルBを用いてICカード101に発行し、PIN管理プログラム132が格納されている専用ファイルを選択しておく。

【0062】次に、カード所有者102が共通PINを決済端末100に入力すると、ステップS703として、決済端末100は、共通PINをICカード101に送信し、ICカード101から個別PINを返信してもらう。この処理では、決済端末100は論理チャンネルBを用いて、個別PIN取得コマンドを、PIN管理プログラム132に発行する。ここで、個別PIN取得コマンドには共通PIN、サービスプログラム131に対応するアプリケーション識別子AID、および取得したい個別PINがオンライン用かオフライン用かを表すフラグが格納されるものとする。PIN管理プログラム132はこれらのデータを取得すると、第1の実施形態で図4を用いて説明した処理手順に従って、個別PINを抽出し、決済端末100に返信する。

【0063】次に、ステップS704として、決済端末100は、PIN認証をオフラインで行なうかオンラインで行なうかをチェックする。

【0064】もし、オフラインPIN認証を行なうなら、ステップS705として、決済端末100は取得した個別PINをICカード101に送信する。この処理では、決済端末100はPIN検証コマンドをサービスプログラム131に発行することで、ICカード101内部で個別PINの照合を行なわせる。

【0065】一方で、もし、オンライン認証を行なうのなら、ステップS706として、決済端末100は取得した個別PINを、ネットワークを介してセンタに送信する。

【0066】以上説明した手順に従って、オフラインPIN認証あるいはオンラインPIN認証が終了した後、ステップS707として、端末100は残りの決済処理を、ICカード101に特定のコマンド発行するなどして継続していく。

【0067】次に、第3の実施形態について説明する。本実施形態に係わるICカードおよび決済端末の構成、およびICカードに格納される情報の構成は、第2の実施形態で説明した構成と同様である。さらに本実施形態においては、ICカード101に格納されているPIN管理プログラム、あるいは複数のサービスプログラムは、ICカード101内部で、互いにAPDU形式のコマンドを送受信することが可能であるものとする。このような処理は、例えば、ICカード用のオペレーティングシステムとして知られているMULTOSが有する機能の1つである「デレゲーション機能」を用いることで実現できる。

【0068】このデレゲーション機能について図8を用いて説明する。図8において、ICカード101には、プログラムA650と、プログラムB651とが格納されている。まず、決済端末100がプログラムA650に対して、APDU形式のコマンドAを発行すると、プログラムA650は、APDU形式のコマンドBをプログラムB651に発行して、任意の処理をプログラムB651に代行させる。次に、プログラムB651は、代行処理の結果をレスポンスBとしてプログラムA650に返す。そして、レスポンスBの結果を基に、プログラムA650は、決済端末100にレスポンスAを返す。

【0069】以上説明したように、ICカード101内部のあるプログラムが、ICカード101外部からコマンドを受信すると、受信したコマンドに基づいて行なう処理の一部を、ICカード101内部にある他のプログラムにコマンドを送信することで代行させる機能をデレゲーション機能と呼ぶ。

【0070】本実施形態においては、上述したデレゲーション機能を用いるが、ICカードのオペレーティングシステムとしては、MULTOSを用いなくても、デレゲーション機能と同等の機能を有している他のオペレーティングシステムを用いる構成であっても構わない。

【0071】次に、本実施形態に係わる決済端末100の処理フローを説明していく。図9は、カード所有者102が、ICカード101を用いて、決済端末100で決済処理を行なうときのフロー図である。この例では、決済端末100がICカード101に送信するコマンドはAPDU形式を用いるものとする。また、ICカードは、サービスプログラム131とPIN管理プログラム132を格納しており、決済端末100は、サービスプログラム131に発行するコマンドの論理チャンネル番号として論理チャンネルAを用い、PIN管理プログラム132に発行するコマンドの論理チャンネル番号として論理チャンネルBを用いて、同時に通信を行なうものとする。

【0072】まず、ICカード101が決済端末100に挿入されると、ステップS800としてICカードの初期化処理を行なう。この処理では、決済端末100がICカード101にリセット要求を送信し、その後ICカード101からリセット応答を受信するといったことが行なわれる。

【0073】次に、決済端末100は、ステップS801として、カード所有者102の選択等により、ICカード101内に格納されているサービスプログラム131を選択する。この処理では、まず、決済端末100が、ファイル選択コマンドを論理チャンネルAを用いてICカード101に発行することで、サービスプログラム131が格納されている専用ファイルを選択する。つづいて、決済端末100が、特定のコマンドを論理チャンネルAを用いてサービスプログラム131に発行して

いくことで、サービスプログラム131に基づいた処理を、PIN認証が必要になるまで行なっていく。

【0074】ここで、PIN認証を実行する前に、決済端末100は、ステップS802として、ファイル選択コマンドを論理チャンネルBを用いてICカード101に発行し、PIN管理プログラム132が格納されている専用ファイルを選択しておく。

【0075】次に、カード所有者102が共通PINを決済端末100に入力すると、ステップS803として、決済端末100は、共通PINをICカード101に送信し、ICカード101内部でPIN検証を行なわせる。この処理では、まず、決済端末100は、論理チャンネルBを用いて、PIN検証コマンドをPIN管理プログラム132に発行する。ここで、PIN検証コマンドには共通PINと、サービスプログラム131に対応するアプリケーション識別子AIDが格納されるものとする。次に、PIN管理プログラム132はこれらのデータを取得すると、第1の実施形態で図4を用いて説明した処理手順に従って、個別PINを抽出する。次にPIN管理プログラム132は、抽出した個別PINを格納したPIN検証コマンドをサービスプログラム131に発行し、サービスプログラム131に個別PINの照合を行なわせ、照合結果を取得する。そして、PIN管理プログラム132は、照合結果を決済端末100に返信する。ここで、ステップS803の処理は、前述したデレゲーション機能を用いることで実現できる。

【0076】以上説明した手順に従って、PIN認証が終了した後、ステップS804として、端末100は残りの決済処理を、ICカード101に特定のコマンド発行するなどして継続していく。

【0077】次に、第4の実施形態について説明する。まず、本実施形態に係わるICカードおよび決済端末の構成を図10に示す。図10に示した構成は、第1の実施形態の説明で図1に示した構成と同様であるが、PIN入力手段113が指紋読み取り手段190に置き換わった点と、カード所有者102が共通PIN105を記憶しなくてもよい点が異なっている。

【0078】ここで、指紋読み取り手段190は、カード所有者102の指紋を読み取り、指紋情報を抽出する機能を有する。したがって、本実施形態においては、カード所有者102は、PINを決済端末100に入力する代わりに、自分の指紋を指紋読み取り手段190で読み取らせることで、本人認証を行う。

【0079】次に、本実施形態に係わるICカードに格納されている情報の構成を図11に示す。図11に示した構成は、第1の実施形態の説明で図2に示した構成と同様であるが、PIN管理専用ファイル122にPIN管理データ142A、142B、142Cを格納する代わりに、AIDと個別PINから成るデータ144A、144B、144Cと、指紋情報191とを格納してい

10

20

30

40

50

る点が異なっている。ここで、データ 144A を構成する AID は専用ファイル 121A に対応し、個別 PIN は専用ファイル 121A に格納されているサービスプログラム 131A により実行されるオフライン PIN 認証に用いられる。同様に、データ 144B を構成する AID は専用ファイル 121B に対応し、個別 PIN はサービスプログラム 131B により実行されるオフライン PIN 認証に用いられる。また、データ 144C を構成する AID は専用ファイル 121C に対応し、個別 PIN はサービスプログラム 131C により実行されるオンライン PIN 認証に用いられる。また、指紋情報 191 は、カード所有者 102 の指紋に対応した情報である。ここで、データ 144A、144B、144C を外部へ読み出すことは、指紋情報 191 の照合が成功しないと出来ないようになっている。

【0080】次に、本実施形態に係わる決済端末 100 の処理フローを説明していく。図 12 は、カード所有者 102 が、IC カード 101 を用いて、決済端末 100 で決済処理を行う時のフロー図である。図 12 に示したフロー図は、第 2 の実施形態の説明で図 7 に示したフローとステップ S702 まで同様であるが、カード所有者 102 は、共通 PIN を決済端末 100 に入力する代わりに、指紋を決済端末 100 に読み取らせている点異なる。

【0081】すなわち、ステップ S1000 において、決済端末 100 が読み取った指紋は、指紋読み取り手段により指紋情報に変換され、決済端末 100 は指紋情報を、IC カード 101 に送信して IC カード 101 から特定の個別 PIN を返信してもらう。この処理では、決済端末 100 は、個別 PIN 取得コマンドを、PIN 管理プログラム 132 に発行する。ここで、個別 PIN コマンドには、指紋情報とサービスプログラム 131 に対応するアプリケーション識別子が格納されており、PIN 管理プログラム 132 は、個別 PIN コマンドを受信すると、指紋情報の照合を行い、照合が成功した場合に、指定したアプリケーション識別子に対応する個別 PIN を決済端末 100 に返す。決済端末 100 は、この個別 PIN を用いることで、第 2 の実施形態と同様の PIN 認証を行うことが可能になる。

【0082】以上説明したように、本実施形態においては、カード所有者 102 が、IC カード 101 を用いて実行可能ないずれかのサービスを受ける場合において、サービス毎に行う必要のある PIN 認証を、指紋を決済端末 100 に読み取らせるだけで、実行することが可能になる。ここで、カード所有者 102 は指紋を決済端末 100 に読み取らせる代わりに共通 PIN を入力し、IC カード 101 には指紋情報を記録する代わりに共通 PIN を記録しておき、IC カード 101 内で共通 PIN の照合が成功した場合に、IC カードから個別 PIN を読み出せる構成であっても本発明の適用範囲である。

【0083】

【発明の効果】以上説明したように、本発明によれば、IC カード所有者が、複数のサービスに対応した IC カードを用いて各サービスを受ける場合に、サービス毎に行なう必要のある PIN 認証を、共通の PIN を一つ覚えておくだけ、あるいは指紋を読み取らせるだけで実行できる構成にすることで、IC カード所有者の利便性を向上することが可能になる。

【図面の簡単な説明】

【図 1】 本発明の第 1 の実施形態に係わる IC カードおよび端末の構成を示した図。

【図 2】 本発明の第 1 の実施形態に係わる IC カードに格納される情報の構成を示した図。

【図 3】 本発明の第 1 の実施形態に係わる PIN 管理データの構成と生成手順を示した図。

【図 4】 本発明の第 1 の実施形態に係わる PIN 管理データの復号手順を示した図。

【図 5】 本発明の第 1 の実施形態に係わる決済端末の処理フローを示した図。

【図 6】 本発明の第 2 の実施形態に係わるコマンドの構成を示した図。

【図 7】 本発明の第 2 の実施形態に係わる決済端末の処理フローを示した図。

【図 8】 本発明の第 3 の実施形態に係わるプログラム間通信の処理フローを示した図。

【図 9】 本発明の第 3 の実施形態に係わる決済端末の処理フローを示した図。

【図 10】 本発明の第 4 の実施形態に係わる IC カードおよび端末の構成を示した図。

【図 11】 本発明の第 4 の実施形態に係わる IC カードに格納される情報の構成を示した図。

【図 12】 本発明の第 4 の実施形態に係わる決済端末の処理フローを示した図。

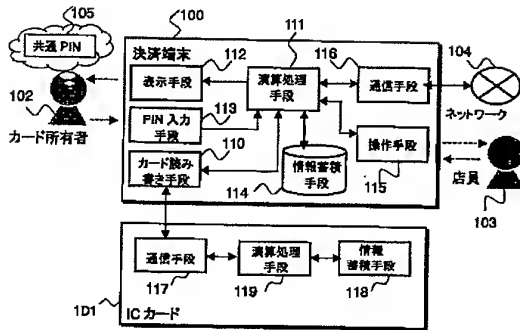
【図 13】 IC カードのファイル構成を示した図。

【符号の説明】

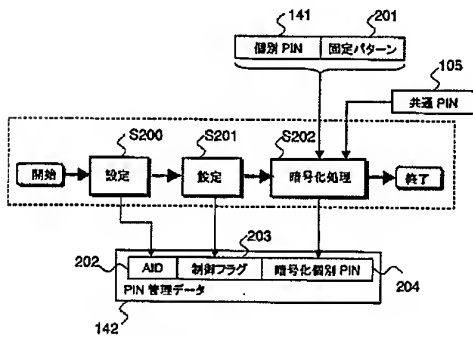
100 決済端末
101 IC カード
102 カード所有者
103 店員
104 ネットワーク
105 共通 PIN
110 カード読み書き手段
111 演算処理手段
112 表示手段
113 PIN 入力手段
114 情報蓄積手段
115 操作手段
116 通信手段
117 通信手段
118 情報蓄積手段

119 演算処理手段

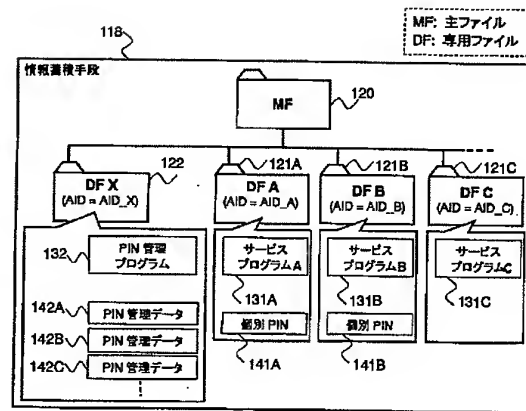
【図1】



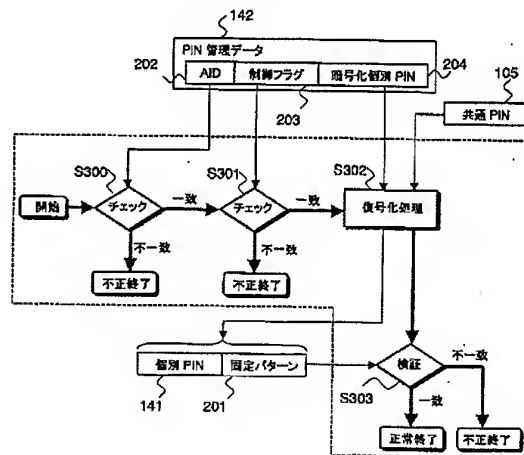
【図3】



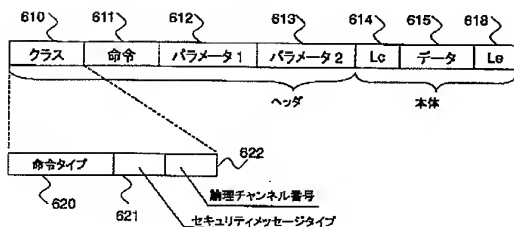
【図2】



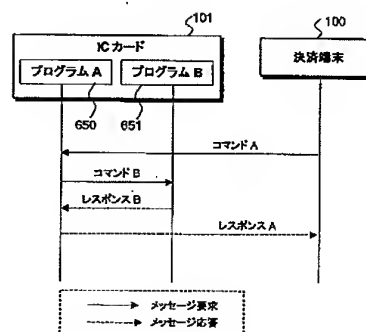
【図4】



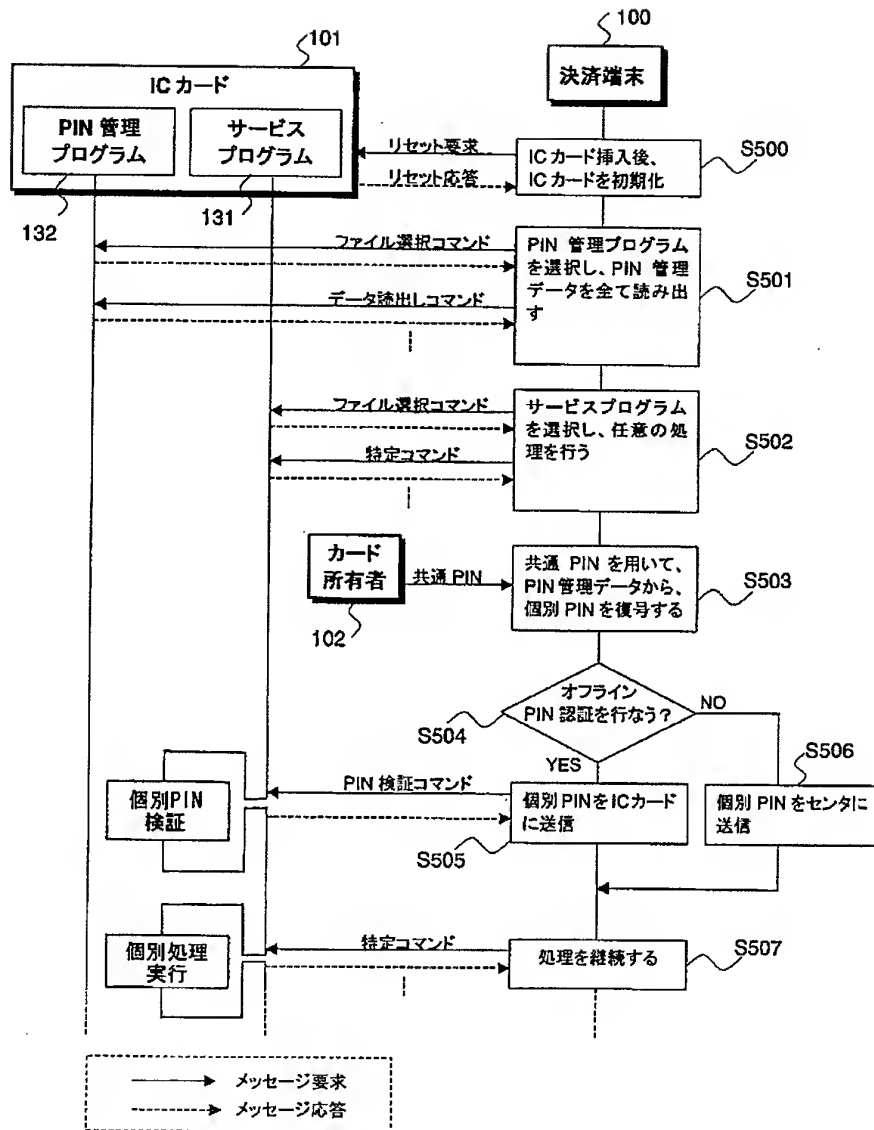
【図6】



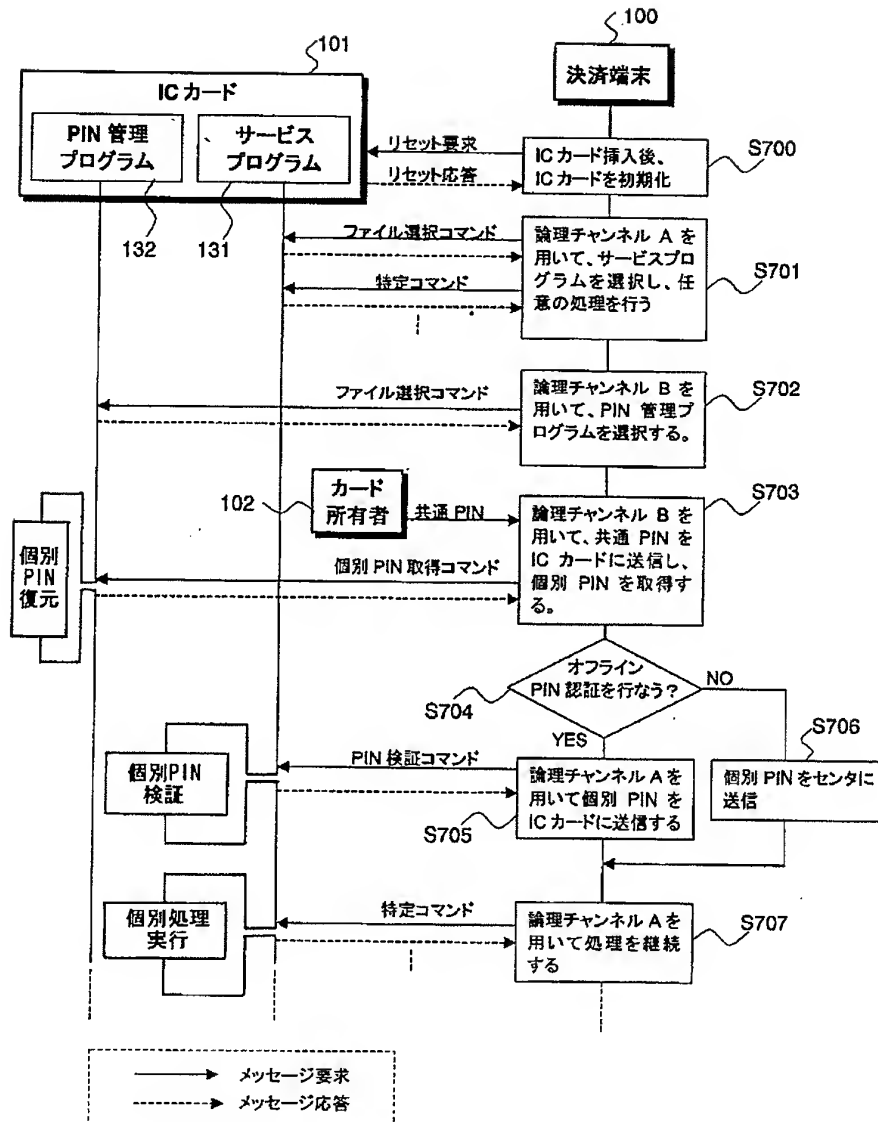
【図8】



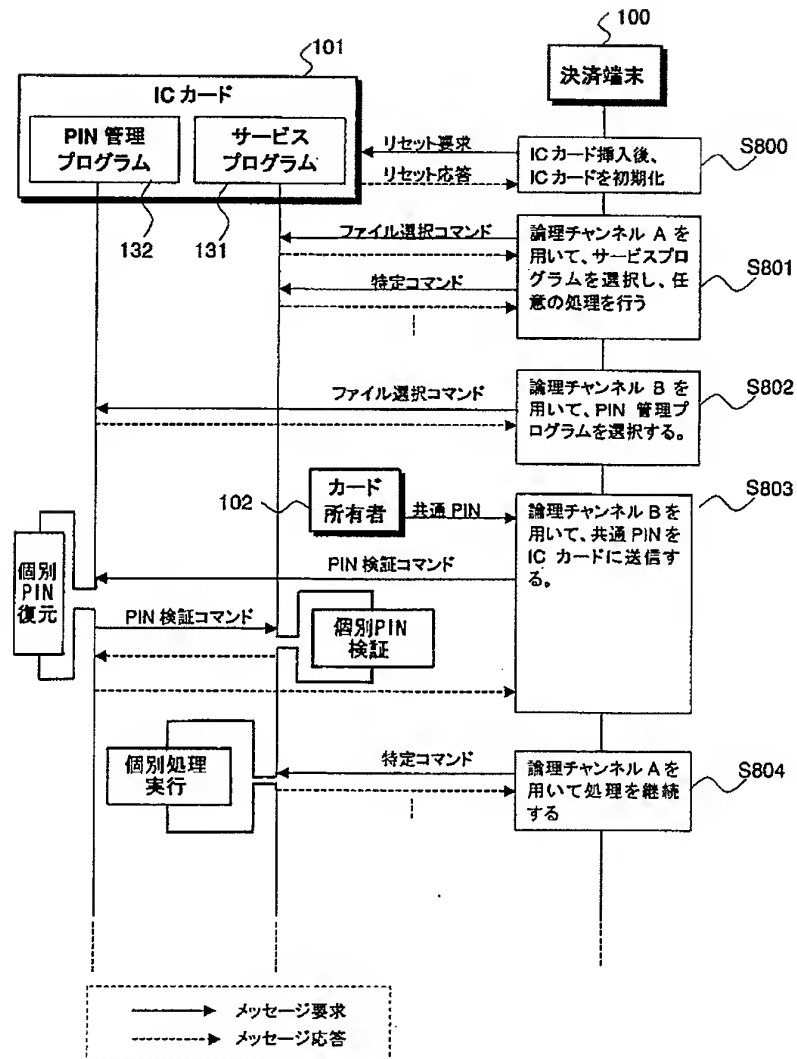
【図5】



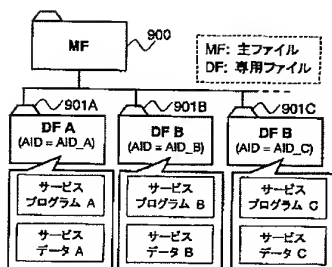
【図7】



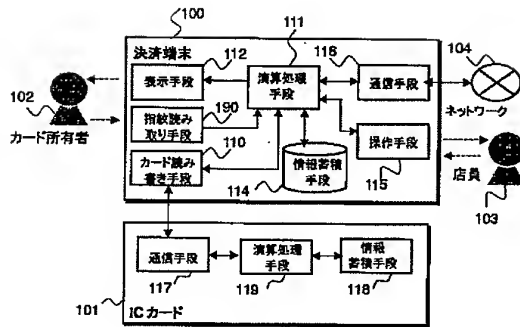
【図9】



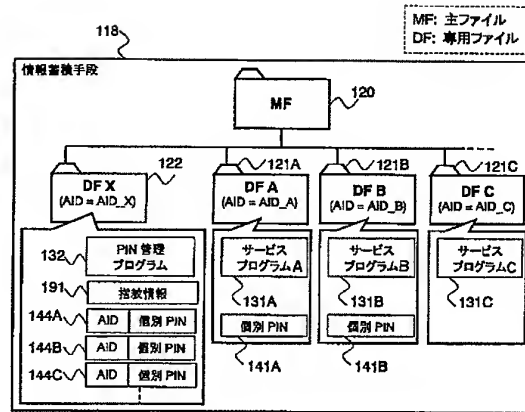
【図13】



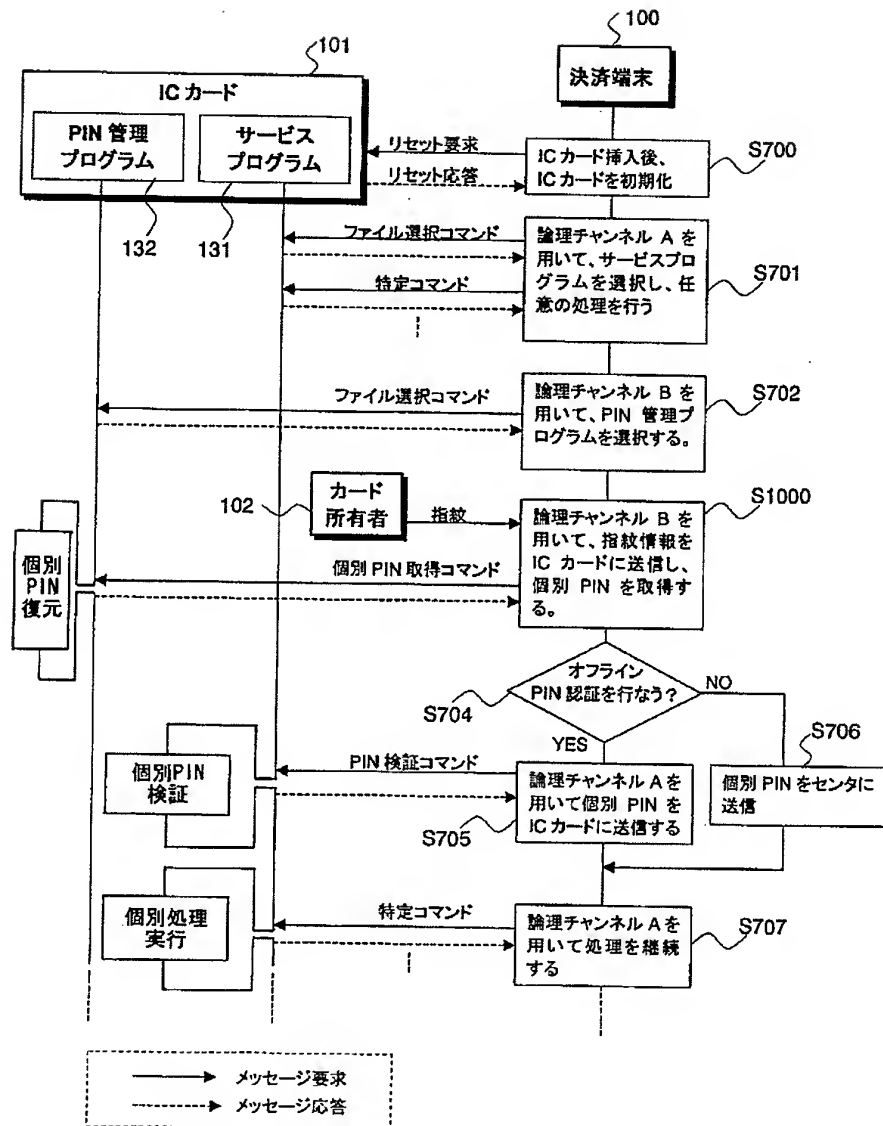
【図10】



【図11】



【図12】



フロントページの続き

(51)Int.Cl.⁷
H04L 9/32

識別記号

FI
H04L 9/00

テマコード(参考)

673E

(72)発明者 高見 穰
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内

(72)発明者 工藤 善道
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内

F ターム(参考) 5B035 AA14 BB09 CA11 CA38
5B058 CA27 KA02 KA04 KA33 KA35
KA37 YA02
5B085 AE01 AE04 AE12 AE23
5J104 AA07 KA01 NA35

CLAIMS

[Claim(s)]

[Claim 1]A service program to process service which needs a cardholder's justification check One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, A password inputting means as which it is an IC card terminal using an IC card one or more encryption passwords which enciphered said individual password were remembered to be, and said cardholder can input the 1st password, A card write means which communicates with said IC card, and said encryption password are read from said IC card by said card write means, Decrypt by said 1st password and it has an arithmetic processing means which transmits the 2nd password that generated and generated the 2nd password to said IC card by said card write means, An IC card terminal characterized by carrying out normal execution of said service when said 2nd password is in agreement with said individual password inside said IC card.

[Claim 2]Establish an information accumulation means which accumulates information acquired from said IC card, and said encryption password is read from said IC card by said card write means, The IC card terminal according to claim 1 reading said encryption password which was accumulated in this information accumulation means and accumulated in this information accumulation means, and decoding by the 1st password.

[Claim 3]Said encryption password enciphers using said 1st password, and what combined fixed value data which consists of as specific a value as said individual password said arithmetic processing means, If said fixed value data corrects to data which decrypted said encryption password using said 1st password and ** is contained in it, said said 2nd password produced by decrypting, The IC card terminal according to claim 1 or 2 judging that it is equal to said individual password.

[Claim 4]A service program to process service which needs a cardholder's justification check One or more pieces, An IC card one or more encryption passwords which enciphered an individual password used in order to perform said cardholder's justification check were remembered to be is used, A password inputting means as which it is an IC card terminal which communicates with a center apparatus which is keeping said individual password, and said cardholder can input the 1st password, A card write means which communicates with said IC card, and a means of communication which communicates with said center apparatus via a network, Said encryption password read from said IC card by said card write means is decrypted by said 1st password, An IC card terminal characterized by carrying out normal execution of said service when the 2nd password is generated, it has an arithmetic processing means which transmits said 2nd password to said center apparatus by said means of communication and said 2nd password is in agreement with said individual password with said center apparatus.

[Claim 5] Establish an information accumulation means which accumulates information acquired from said IC card, and said encryption password is read from said IC card by said card write means, The IC card terminal according to claim 4 reading said encryption password which was accumulated in this information accumulation means and accumulated in this information accumulation means, and decoding by the 1st password.

[Claim 6] Said encryption password enciphers using said 1st password, and what combined fixed value data which consists of as specific a value as said individual password said arithmetic processing means, The IC card terminal according to claim 5 which will be characterized by judging that said said 2nd password produced by decrypting is equal to said individual password if said fixed value data corrects to data which decrypted said encryption password using said 1st password and ** is contained in it.

[Claim 7] A service program to process service which needs a cardholder's justification check One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, An IC card one or more encryption passwords which enciphered said individual password were remembered to be, the person himself/herself in a system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- it being an authentication method and, A processing step to which said IC card terminal reads said encryption password from said IC card, A processing step which accumulates said encryption password which said IC card terminal read from said IC card, A processing step as which said card holder inputs the 1st password into said IC card terminal, A processing step which decrypts said encryption password which said IC card terminal is accumulating by said 1st password, and generates the 2nd password, the person himself/herself by whom a processing step which carries out normal execution of said service being included when said IC card terminal transmits said 2nd password to said IC card and said 2nd password is in agreement with said individual password inside said IC card -- an authentication method.

[Claim 8] A service program to process service characterized by comprising the following which needs a cardholder's justification check One or more pieces, An IC card one or more encryption passwords which enciphered an individual password used in order to perform said cardholder's justification check were remembered to be, the person himself/herself in a system which consists of a center apparatus which is connected with an IC card terminal which provides said service for said cardholder using said IC card, and said IC card terminal via a network, and is keeping said individual password -- an authentication method.
A processing step to which said IC card terminal reads said encryption password from said IC card.

A processing step which accumulates said encryption password which said IC card terminal read from said IC card.

A processing step as which said card holder inputs the 1st password into said IC card terminal. A processing step which decrypts said encryption password which said IC card terminal is accumulating by said 1st password, and generates the 2nd password, A processing step which carries out normal execution of said service when said IC card terminal transmits said 2nd password to said center apparatus and said 2nd password is in agreement with said individual password with said center apparatus.

[Claim 9]A service program to process service which needs a cardholder's justification check One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, An IC card a password control program in which an encryption password which enciphered said individual password manages one or more pieces and said encryption password was remembered to be, the person himself/herself in a system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- with a processing step as which it is an authentication method and said cardholder inputs the 1st password into said IC card terminal. A processing step at which said IC card terminal transmits said 1st password to said IC card, Said password control program executed within said IC card decrypts said encryption password by said 1st password, and generates the 2nd password, A processing step which transmits to said IC card terminal, and said IC card terminal transmit said 2nd password to said IC card, the person himself/herself by whom a processing step which carries out normal execution of said service being included when said 2nd password is in agreement with said individual password inside said IC card -- an authentication method.

[Claim 10]A service program to process service which needs a cardholder's justification check One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, An IC card a password control program in which an encryption password which enciphered said individual password manages one or more pieces and said encryption password was remembered to be, the person himself/herself in a system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- with a processing step as which it is an authentication method and said card holder inputs the 1st password into said IC card terminal. A processing step at which said IC card terminal transmits said 1st password to said IC card, A processing step which said password control program executed within said IC card decrypts said encryption password by said 1st password, and generates the 2nd password, the person himself/herself by whom a processing step which carries out normal execution of said service being included when said password program transmits the 2nd password to said service program and said 2nd password is in agreement with said individual password -- an authentication method.

[Claim 11]A service program to process service characterized by comprising the following

which needs a cardholder's justification check One or more pieces, An IC card terminal which provides said service for said cardholder using an IC card the 1st password that protects that an individual password used in order to perform said cardholder's justification check outputs one or more pieces and said individual password outside was remembered to be.

A password inputting means as which said cardholder can input the 2nd password.

A card write means which communicates with said IC card.

Transmit to said IC card by said IC card write means, and said 2nd password inside said IC card, When said 2nd password is in agreement with said 1st password, acquire said individual password by said IC card write means, and said individual password is transmitted to said IC card by said card write means, An arithmetic processing means which carries out normal execution of said service when collation of said individual password inside said IC card is successful.

[Claim 12]A service program to process service characterized by comprising the following which needs a cardholder's justification check One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, An IC card terminal which provides said service for said cardholder using an IC card the 1st biological information that protects outputting said individual password outside, and a control program which manages biological information were remembered to be.

A biological information reading means which can read the 2nd biological information in said cardholder.

A card write means which communicates with said IC card.

Transmit said 2nd biological information to said IC card by said IC card write means, and inside said IC card, When said 2nd biological information is in agreement with said 1st biological information, acquire said individual password by said IC card write means, and said individual password is transmitted to said IC card by said card write means, An arithmetic processing means which carries out normal execution of said service when collation of said individual password inside said IC card is successful.

[Claim 13]The IC card terminal according to claim 12, wherein a fingerprint is used for said 1st biological information and said 2nd biological information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]an IC card is used for this invention -- the person himself/herself -- it is related with the IC card terminal equipment and the person-himself/herself authentication method which attest.

[0002]

[Description of the Prior Art]In recent years, an IC card is spreading widely instead of a magnetic card. This is because there is the feature provided with the arithmetic unit (microprocessor) for performing cipher processing with a large storage capacity, etc. which is not in a magnetic card that an inside can be observed easily and nothing is (it has the Tampa-proof nature) in an IC card. By applying an IC card with such a feature to a settlement system, an identification system, etc., security can be raised compared with a magnetic card, or the new service which was not able to be realized in a magnetic card can be provided. For example, there are electronic money and a credit card as service which a settlement system provides, and an employee ID card, a driver's license, etc. are raised as service which an identification system provides.

[0003]The IC card is classified into the contact type and the noncontact type according to the communication method.

Each specification is already standardized.

For example, a contact smart card is ISO (International Organization for Standardization: International Organization for Standardization), and is standardized as ISO/IEC7816. The IC card based on ISO/IEC7816 calculates inside according to the command which transmits from a terminal, is performing returning a result as a response one by one, and carries out processing for realizing service.

[0004]Here, the command and response which are transmitted and received between IC card terminals are specified in the form of APDU (Application Protocol Data Unit) ISO/IEC7816. The IC card based on ISO/IEC7816 is stored in the file in which a program and data had a layered structure as shown in drawing 13.

[0005]In drawing 13, the main file (MF) 900 is a file of a top layer, and exists only one in an IC card, and two or more dedicated file (DF)901A, and 901B and 901C exist in the bottom of it. Data (it is called service information below) required for the program (it is called the service program below) and service execution for performing specific service is stored in a dedicated file. Since two or more existence is possible for a dedicated file in an IC card, two or more services can be used by the IC card of one sheet by storing two or more service programs and service information in a different dedicated file.

[0006]In order to execute a specific service program, a terminal chooses first the dedicated file in which the specific service program is stored as a file of KARENTO using the "file selection command" specified as a command of APDU form. Thereby, the command which an IC card receives from a terminal after it comes to be processed according to the selected service program. Here, each dedicated file is identifiable from the outside by ID called an application identifier (it omits the following AID). For example, the "file selection command" can choose a specific dedicated file by specifying AID.

[0007]now, the case where service is received using an IC card -- a cardholder -- the attestation which it may be urged to attest that the person himself/herself is using that card, for this reason it performs -- the person himself/herself -- it is called attestation. The PIN attestation as which a cardholder inputs the password called PIN into a terminal as a method for realizing person-himself/herself attestation is common. PIN attestation includes "off-line PIN attestation" compared with PIN which has memorized PIN which the cardholder inputted in an IC card, and "on-line PIN attestation" compared with PIN in which the center holds PIN which the cardholder inputted via a network. the persons themselves himself/herself, such as PIN attestation, -- attesting is important in order to prevent the illegal use of an IC card.

[0008]

[Problem to be solved by the invention]As explained above, can use various services by the IC card of one sheet by using an IC card, but. On the other hand, in order to use each service, when performing PIN attestation, the cardholder keeps different PIN for every service in mind, and may have to use PIN properly for every service to be used. This becomes a factor which spoils a card user's convenience greatly.

[0009]Then, when this invention receives each service using an IC card corresponding to two or more services in an IC card owner, an IC card terminal which can improve an IC card owner's convenience by carrying out PIN attestation which needs to be performed for every service to composition which can be performed only by keeping one common PIN in mind, and the person himself/herself -- it aims at providing an authentication method.

[0010]

[Means for solving problem]In this invention, a service program to process service which needs a cardholder's justification check To achieve the above objects, one or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, A password inputting means as which said cardholder can input the 1st password in an IC card terminal using an IC card one or more encryption passwords which enciphered said individual password were remembered to be, A card write means which communicates with said IC card, and an information accumulation means which accumulates information acquired from said IC card, Said encryption password is read from said IC card by said card write means, Said encryption password which was accumulated in said information accumulation

means and accumulated in said information accumulation means is read, Decrypt by said 1st password, generate the 2nd password, and said 2nd password is transmitted to said IC card by said card write means, When said 2nd password is in agreement with said individual password inside said IC card, it has an arithmetic processing means which carries out normal execution of said service.

[0011]In this invention, the service program to process the service which needs a cardholder's justification check One or more pieces, The individual password used in order to perform said cardholder's justification check One or more pieces, The IC card one or more encryption passwords which enciphered said individual password were remembered to be, the person himself/herself in the system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- an authentication method with the processing step to which said IC card terminal reads said encryption password from said IC card. The processing step which accumulates said encryption password which said IC card terminal read from said IC card, The processing step as which said card holder inputs the 1st password into said IC card terminal, The processing step which decrypts said encryption password which said IC card terminal is accumulating by said 1st password, and generates the 2nd password, When said IC card terminal transmits said 2nd password to said IC card and said 2nd password is in agreement with said individual password inside said IC card, the processing step which carries out normal execution of said service is included.

[0012]Namely, in order to solve an aforementioned problem, this invention, The service program to process the service which needs a cardholder's justification check One or more pieces, The individual password used in order to perform said cardholder's justification check One or more pieces, The password inputting means as which said cardholder can input the 1st password in the IC card terminal using the IC card one or more encryption passwords which enciphered said individual password were remembered to be, The card write means which communicates with said IC card, and said encryption password are read from said IC card by said card write means, Decrypt by said 1st password and it has an arithmetic processing means which transmits the 2nd password that generated and generated the 2nd password to said IC card by said card write means, When said 2nd password was in agreement with said individual password inside said IC card, it was made to carry out normal execution of said service.

[0013]This invention establishes an information accumulation means which accumulates information acquired from said IC card in the above-mentioned IC card terminal, and reads said encryption password from said IC card by said card write means, Said encryption password which was accumulated in this information accumulation means and accumulated in this information accumulation means is read, and it was made to decode by the 1st password.

[0014]In the above-mentioned IC card terminal, this invention said encryption password,

Encipher using said 1st password and what combined said individual password and fixed value data which consists of a specific value said arithmetic processing means, When said fixed value data corrected to data which decrypted said encryption password using said 1st password and ** was contained in it, we decided to judge that said said 2nd password produced by decrypting is equal to said individual password.

[0015]In order to solve an aforementioned problem, a service program which processes service which needs a cardholder's justification check this invention One or more pieces, An IC card one or more encryption passwords which enciphered an individual password used in order to perform said cardholder's justification check were remembered to be is used, A password inputting means as which said cardholder can input the 1st password in an IC card terminal which communicates with a center apparatus which is keeping said individual password, A card write means which communicates with said IC card, and a means of communication which communicates with said center apparatus via a network, Said encryption password read from said IC card by said card write means is decrypted by said 1st password, When the 2nd password was generated, it had an arithmetic processing means which transmits said 2nd password to said center apparatus by said means of communication and said 2nd password was in agreement with said individual password with said center apparatus, we decided to carry out normal execution of said service.

[0016]This invention establishes an information accumulation means which accumulates information acquired from said IC card in the above-mentioned IC card terminal, and reads said encryption password from said IC card by said card write means, Said encryption password which was accumulated in this information accumulation means and accumulated in this information accumulation means is read, and it was made to decode by the 1st password.

[0017]In the above-mentioned IC card terminal, this invention said encryption password, Encipher using said 1st password and what combined said individual password and fixed value data which consists of a specific value said arithmetic processing means, When said fixed value data corrected to data which decrypted said encryption password using said 1st password and ** was contained in it, we decided to judge that said said 2nd password produced by decrypting is equal to said individual password.

[0018]In order to solve an aforementioned problem, a service program which processes service which needs a cardholder's justification check this invention One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, An IC card one or more encryption passwords which enciphered said individual password were remembered to be, the person himself/herself in a system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- an authentication method with a processing step to which said IC card terminal reads said encryption password from said IC card. A processing step which accumulates said encryption

password which said IC card terminal read from said IC card, A processing step as which said card holder inputs the 1st password into said IC card terminal, A processing step which decrypts said encryption password which said IC card terminal is accumulating by said 1st password, and generates the 2nd password, When said IC card terminal transmitted said 2nd password to said IC card and said 2nd password was in agreement with said individual password inside said IC card, it was made for a processing step which carries out normal execution of said service to be included.

[0019]In order to solve an aforementioned problem, the service program which processes the service which needs a cardholder's justification check this invention One or more pieces, The IC card one or more encryption passwords which enciphered the individual password used in order to perform said cardholder's justification check were remembered to be, The IC card terminal which provides said service for said cardholder using said IC card, the person himself/herself in the system which consists of a center apparatus which is connected with said IC card terminal via the network, and is keeping said individual password -- an authentication method, The processing step to which said IC card terminal reads said encryption password from said IC card, The processing step which accumulates said encryption password which said IC card terminal read from said IC card, The processing step as which said card holder inputs the 1st password into said IC card terminal, The processing step which decrypts said encryption password which said IC card terminal is accumulating by said 1st password, and generates the 2nd password, When said IC card terminal transmits said 2nd password to said center apparatus and said 2nd password is in agreement with said individual password with said center apparatus, It was made for the processing step which carries out normal execution of said service to be included.

[0020]In order to solve an aforementioned problem, the service program which processes the service which needs a cardholder's justification check this invention One or more pieces, The individual password used in order to perform said cardholder's justification check One or more pieces, The IC card the password control program in which the encryption password which enciphered said individual password manages one or more pieces and said encryption password was remembered to be, the person himself/herself in the system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- an authentication method with the processing step as which said cardholder inputs the 1st password into said IC card terminal. The processing step at which said IC card terminal transmits said 1st password to said IC card, Said password control program executed within said IC card decrypts said encryption password by said 1st password, and generates the 2nd password, It was made for the processing step which transmits to said IC card terminal, and the processing step which carries out normal execution of said service when said IC card terminal transmits said 2nd password to said IC card and said 2nd password is in agreement

with said individual password inside said IC card to be included.

[0021]In order to solve an aforementioned problem, the service program which processes the service which needs a cardholder's justification check this invention One or more pieces, The individual password used in order to perform said cardholder's justification check One or more pieces, The IC card the password control program in which the encryption password which enciphered said individual password manages one or more pieces and said encryption password was remembered to be, the person himself/herself in the system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- an authentication method with the processing step as which said card holder inputs the 1st password into said IC card terminal. The processing step at which said IC card terminal transmits said 1st password to said IC card, The processing step which said password control program executed within said IC card decrypts said encryption password by said 1st password, and generates the 2nd password, When said password program transmitted the 2nd password to said service program and said 2nd password was in agreement with said individual password, it was made for the processing step which carries out normal execution of said service to be included.

[0022]This invention is provided with the following in order to solve an aforementioned problem.

A service program which processes service which needs a cardholder's justification check is one or more pieces.

An individual password used in order to perform said cardholder's justification check is one or more pieces.

A password inputting means as which said cardholder can input the 2nd password in an IC card terminal which provides for said cardholder the **** aforementioned service for IC cards the 1st password that protects outputting said individual password outside was remembered to be.

Transmit to said IC card by said IC card write means, and a card write means which communicates with said IC card, and said 2nd password inside said IC card, When said 2nd password is in agreement with said 1st password, acquire said individual password by said IC card write means, and said individual password is transmitted to said IC card by said card write means, An arithmetic processing means which carries out normal execution of said service when collation of said individual password inside said IC card is successful.

[0023]This invention is provided with the following in order to solve an aforementioned problem.

A service program which processes service which needs a cardholder's justification check is one or more pieces.

An individual password used in order to perform said cardholder's justification check is one or more pieces.

The 1st biological information that protects outputting said individual password outside.

A biological information reading means in which an IC card terminal which provides said service for said cardholder using an IC card a control program which manages biological information was remembered to be can read the 2nd biological information in said cardholder, Transmit a card write means which communicates with said IC card, and said 2nd biological information to said IC card by said IC card write means, and inside said IC card, When said 2nd biological information is in agreement with said 1st biological information, acquire said individual password by said IC card write means, and said individual password is transmitted to said IC card by said card write means, An arithmetic processing means which carries out normal execution of said service when collation of said individual password inside said IC card is successful.

[0024]In the above-mentioned IC card terminal, the fingerprint was used for this invention as said 1st biological information and said 2nd biological information.

[0025]

[Mode for carrying out the invention]Hereafter, the embodiment of this invention is described. Although following embodiments explain the case where the IC card of a contact type is used, it is not an item required for this invention that it is a contact type, for example, this invention is here, applicable even if it is a noncontact IC card. In following embodiments, although the command transmitted and received between a terminal and an IC card assumes the command of APDU form, If it is a command set which it is not an item required for this invention to use the command of APDU form, and can realize a function equivalent to APDU form, this invention is applicable no matter what thing it may use. not the item in which it is required for this invention to be such a terminal although the terminal with the function to perform the settlement of accounts for electronic money or a credit card as a terminal is assumed in following embodiments but the person himself/herself -- this invention is applicable if it is a terminal which attests.

[0026]First, a 1st embodiment is described. drawing 1 -- the person himself/herself -- the composition of the IC card and terminal concerning this embodiment which attests is shown. in drawing 1 -- the person himself/herself -- attestation is performed between the settlement system 100, IC card 101, the cardholder 102, the salesclerk 103, and the network 104. The composition shown in drawing 1 assumes that the cardholder 102 performs the settlement of accounts by electronic money or a credit card using IC card 101. Therefore, the settlement system 100 is a terminal provided with the clearing function by an IC card, for example, assumes ATM of a credit terminal or a financial institution. IC card 101 has the composition

that service of plurality, such as electronic money and a credit card, can be provided. the cardholder 102 -- the person himself/herself -- suppose that common PIN105 which can be used in common with two or more services which are PIN used for attestation and IC card 101 provides is memorized.

[0027]Next, the internal configuration of the settlement system 100 is explained. The settlement system 100 has the card write means 110, the arithmetic processing means 111, the display device 112, the PIN input means 113, the information accumulation means 114, the control means 115, and the means of communication 116.

[0028]The card write means 110 has the function to transmit a command to IC card 101 (writing), or to receive a response from an IC card (reading), in order to communicate with IC card 101.

[0029]The arithmetic processing means 111 comprises a microprocessor and a program storing memory, for example, controls the settlement system 100 whole based on the program stored in the program storing memory, and has a function which carries out settling processing.

[0030]The displaying means 112 displays the variety of information of a settlement amount etc. as opposed to the cardholder 102.

[0031]the PIN input means 113 -- the cardholder 102 -- the person himself/herself -- it has a function in which PIN for attestation can be inputted, for example using a ten key etc.

[0032]The information accumulation means 114 has a function which accumulates temporarily or permanently the information acquired from IC card 101 or the network 104, or the information which the cardholder 102 and the salesclerk 103 inputted, for example, comprises a hard disk, semiconductor memory, etc.

[0033]The control means 115 provides Interface Division for the salesclerk 103 to operate the settlement system 100, for example, comprises a keyboard, a bar code reader, a display, etc.

[0034]The means of communication 116 is used in order to have a function which communicates with a center via the network 104, for example, to perform on-line PIN attestation. Here, in the case of unmanned terminals, such as financial institution ATM, the control means 115 may not be, and, in the salesclerk 103, the settlement system 100 does not need to exist. When the settling processing by the settlement system 100 is completed off-line, there may not be the means of communication 116.

[0035]Next, the internal configuration of IC card 101 is explained. IC card 101 has the means of communication 117, the information accumulation means 118, and the arithmetic processing means 119.

[0036]The means of communication 117 communicates with the card write means 110 of the settlement system 100, and has the function to receive a command from the settlement system 100, or to reply a response to the settlement system 100.

[0037]The program and data in which the information accumulation means 118 performs service which an IC card provides, Or it has the function to store the information etc. which were acquired from the settlement system 100 temporarily or permanently, for example, comprises semiconductor memory, such as ROM (Read Only Memory), RAM (Random Access Memory), and a flash memory.

[0038]The arithmetic processing means 119 is using a microprocessor, manages control of the whole IC card and has the function to execute the program stored in the information accumulation means 118.

[0039]Next, the composition of the information stored in IC card 101 concerning this embodiment is shown in drawing 2. Drawing 2 is the file organization of information accumulation means 118 inside which constitutes IC card 101, and comprises the main file (MF) 120, dedicated file (DF)121A, 121B and 121C, and the PIN management dedicated file 122. These files have a layered structure and have the composition that the main file 120 is located in the top and the dedicated files 121A, 121B, and 121C and the PIN management dedicated file 122 are located in the lower layer. Different AID is assigned to each dedicated file and it is identifiable from the outside.

[0040]Next, an internal configuration of the dedicated files 121A, 121B, and 121C is explained. in the service program 131A which performs specific account settlement services in the dedicated file 121A, and these account settlement services -- the person himself/herself -- individual PIN141A which is data required in order to perform attestation by off-line PIN attestation is stored. The service program 131B and individual PIN141B are similarly stored in the dedicated file 121B. account settlement services which the service program 131C is stored in the dedicated file 121C, and are performed by the service program 131C -- the person himself/herself -- on-line PIN attestation shall be performed as attestation Therefore, PIN data is not stored in the dedicated file 121C.

[0041]Next, the PIN management dedicated file 122 is explained. The PIN management dedicated file 122 is a dedicated file for PIN management. The PIN control program 132 which manages individual PIN individually used for the PIN management dedicated file 122 with the service programs 131A, 131B, and 131C, The PIN management data 142A, 142B, and 142C which is data which the PIN control program 132 manages is stored. Data which needs the PIN management data 142A for off-line PIN attestation performed by the service program 131A here is contained. Similarly, data which needs the PIN management data 142B for off-line PIN attestation performed by the service program 131B is contained. Data which needs the PIN management data 142C for on-line PIN attestation performed by the service program 131C is contained.

[0042]Although three service programs are contained in the information accumulation means 118 and an PIN control program has composition of having managed three PIN management

data, in this explanation, this invention is applicable also to an IC card in which arbitrary numbers of service programs are contained. For example, when IC card 101 contains four service programs, the PIN control program should just manage four PIN management data. This invention is applicable even if it is the composition of performing off-line PIN attestation even if a service program in IC card 101 is the composition of performing on-line PIN attestation.

[0043]Next, composition and the directions for PIN management data which the PIN control program 132 concerning this embodiment has managed are explained. First, composition and a generation procedure of PIN management data are shown in drawing 3. In drawing 3, the PIN management data 142 has AID202, the control flag 203, and composition that encryption individual PIN204 is contained. AID202 is an application identifier of a dedicated file in which a service program with which the PIN management data 142 corresponds is stored. The control flag 203 shows an PIN authentic method (on-line or off-line) with which the PIN management data 142 corresponds. For example, 1 bit shall be assigned to the control flag 203 and, in the case of individual PIN for on-line in a case of "0", and "1", individual PIN for off-line shall be held at the PIN management data 142. Encryption individual PIN204 enciphers individual PIN and the contents of original individual PIN cannot be guessed only from encryption individual PIN204.

[0044]As a generation procedure of the PIN management data 142, right AID202 is first set up as Step S200. Next, the right control flag 203 is set up as Step S201. Next, encryption processing is performed by using as an encryption key common PIN105 to which the cardholder set the data which combined individual PIN141 and the fixed pattern 201 as Step S202, and the cryptogram outputted is set to encryption individual PIN204. Here, the fixed pattern 201 is a certain specific bit string, and is defined as a fixed value. It is possible to use DES which is a cryptographic algorithm based on a block cipher system, for example as encryption processing performed at Step S202. Or other encryption algorithms may be used.

[0045]The above generation procedure is performed, when registering the PIN management data 142 newly and changing common PIN105, and when changing individual PIN141. What is necessary is just to replace with old PIN management data the PIN management data generated by new common PIN, when changing common PIN. What is necessary is similarly, just to replace with old PIN management data the PIN management data generated from new individual PIN, when changing individual PIN.

[0046]Next, the procedure which extracts individual PIN from PIN management data is shown in drawing 4. This procedure is performed by using the arithmetic processing means 111 which constitutes the settlement system 100 shown in drawing 1. In drawing 4, the PIN management data 142 has AID202, the control flag 203, and the composition that encryption individual PIN204 is contained, as mentioned above.

[0047]First, it is investigated whether it is in agreement with the application identifier of the dedicated file in which the service program which checks AID202 and uses individual PIN as Step S300 is stored. If AID is not in agreement, the end of this processing of unjust is carried out. If AID is in agreement, next, as Step S301, the control flag 203 will be checked and it will be investigated whether the control flag 203, the shown PIN authentic method (off-line or on-line), and the PIN authentic method which the service program which uses individual PIN holds are in agreement. If a PIN authentic method is not in agreement, the end of the processing of unjust is carried out. When a PIN authentic method is in agreement, next, as Step S302, by using common PIN105 as an encryption key, decoding processing is performed and the plaintext outputted is divided into individual PIN141 and the fixed pattern 201. Here, as common PIN105, the cardholder 102 uses what was inputted into the terminal 100.

[0048]Next, it is verified whether the acquired fixed pattern 201 is a right value as Step S303. Here, the terminal 100 presupposes that the right value of a fixed pattern is known beforehand. If the fixed pattern 201 is not a right value, the end of this processing of unjust will be carried out. If the fixed pattern 201 is a right value, it will consider that individual PIN141 has been acquired correctly and normal termination of this processing will be carried out.

[0049]Next, the process flow of the settlement system 100 concerning this embodiment is explained. Drawing 5 is a flow chart in case the cardholder 102 performs settling processing with the settlement system 100 using IC card 101. Here, this settling processing shall be performed using the arithmetic processing means 111 which constitutes the settlement system 100 shown by drawing 1. In this example, although the IC card stores the service program 131 and the PIN control program 132, the settlement system 100 shall not communicate simultaneously with two or more programs stored in IC card 101. The command which the settlement system 100 transmits to IC card 101 is explained as what uses APDU form.

[0050]First, if IC card 101 is inserted in the settlement system 100, initialization processing of an IC card will be performed as Step S500. In this processing, the settlement system 100 transmits a reset request to IC card 101, and receiving a reset response from IC card 101 after that is performed. Next, the settlement system 100 reads all the PIN management data stored in IC card 101 as Step S501. In this processing, the settlement system 100 chooses first the PIN management dedicated file in which the PIN control program 132 is stored by publishing a file selection command to IC card 101. The PIN management data 142 is altogether read because continue and the settlement system 100 publishes a data readout command to the PIN control program 132. The read PIN management data is stored in the information accumulation means 114 shown in drawing 1.

[0051]Next, the terminal 100 chooses the service program 131 stored in IC card 101 by the cardholder's 102 selection, etc. as Step S502. In this processing, the settlement system 100 chooses first the dedicated file in which the service program 131 is stored by publishing a file

selection command to IC card 101. It continues, and by publishing a command with the specific settlement system 100 to the service program 131, processing based on the service program 131 is performed until PIN attestation is needed.

[0052]Next, the cardholder's 102 input of common PIN105 will decode individual PIN as Step S503 from PIN management data previously read from an IC card using common PIN inputted into the terminal 100. In this processing, it performs until it succeeds processing which extracts individual PIN explained using drawing 4 to all the PIN management data read from an IC card. Here, if extracting processing of individual PIN ends in failure, an operation method of interrupting settling processing will be considered first. Or if extracting processing of individual PIN goes wrong, an operation method of continuing settling processing after considering that common PIN inputted into the terminal 100 is individual PIN will also be considered. About a case of the latter, the cardholder 102 becomes an operation method in a case of inputting either common PIN or individual PIN as Step S503.

[0053]Next, it confirms whether perform PIN attestation off-line or carry out on-line as Step S504. Supposing it performs off-line PIN attestation, the settlement system 100 will transmit extracted individual PIN to IC card 101 as Step S505. The settlement system 100 is publishing an PIN verification command to the service program 131, transmits individual PIN to IC card 101, and makes individual PIN compare inside in this processing. If one side is also carried out and on-line attestation is performed, the settlement system 100 transmits extracted individual PIN to a center via a network as Step S506. After off-line PIN attestation or on-line PIN attestation is completed according to a procedure explained above, as Step S507, the terminal 100 is specific to IC card 101, carries out command issue of the remaining settling processings to it, and is continued.

[0054]Next, a 2nd embodiment is described. The composition of the IC card and settlement system concerning this embodiment is the same as the composition shown by explanation using drawing 1 by a 1st embodiment. The composition of the information stored in the IC card concerning this embodiment is the same as the composition explained using drawing 2 by a 1st embodiment. The procedure which extracts individual PIN from PIN management data is the same as the procedure explained using drawing 4 by a 1st embodiment. However, according to this embodiment, let the terminal 100 be what has possible communicating with the PIN control program stored in IC card 101, and two or more service programs simultaneously. In this embodiment, the PIN control program 132 stored in IC card 101 shall perform processing which extracts individual PIN from PIN management data.

[0055]Hereafter, a realization method of this embodiment is shown. First, drawing 6 is a block diagram of a command of APDU form. In drawing 6, a command of APUD form comprises the class 610, the command 611, the parameter 1 (612), the parameter 2 (613), Lc614, the data 615, and Le616. The class 610 is an identifier of a service program which communicates using

a command. The command 611 shows an instruction code of a command. The parameter 1 (612) and the parameter 2 (613) store a value of a parameter depending on the command 611. Lc614 expresses the length of the data 615 which is the next field. The data 615 is the field which stores data transmitted to an IC card. Le616 expresses the length of a response returned from an IC card.

[0056]In drawing 6, the class 610 comprises the command type 620, the security message type 621, and the logical channel number 622. The command type 620 is the field for classifying the command 611. A security message type is the field showing whether encryption processing for preventing tapping and an alteration of the data 615 is performed. The logical channel number 622 is used in order to distinguish the command published to the program stored in the IC card using a logical address. That is, it becomes possible by changing the value of the logical channel number 622 to communicate with two or more programs in an IC card simultaneously.

[0057]In the above explanation, although explained taking the case of the command of APDU form, if it has a function equivalent to the function using a logical channel, even if it is a command of other forms, it is applicable to this invention.

[0058]Next, the process flow of the settlement system 100 concerning this embodiment is explained. Drawing 7 is a flow chart in case the cardholder 102 performs settling processing with the settlement system 100 using IC card 101. This example explains the command which the settlement system 100 transmits to IC card 101 as what uses APDU form. The IC card stores the service program 131 and the PIN control program 132, and the settlement system 100, It shall communicate simultaneously, using logical channel B as a logical channel number of the command published to the PIN control program 132 using logical channel A as a logical channel number of the command published to the service program 131.

[0059]First, if IC card 101 is inserted in the settlement system 100, initialization processing of an IC card will be performed as Step S700. In this processing, the settlement system 100 transmits a reset request to IC card 101, and receiving a reset response from IC card 101 after that is performed.

[0060]Next, the settlement system 100 chooses the service program 131 stored in IC card 101 by the cardholder's 102 selection, etc. as Step S701. In this processing, the dedicated file in which the service program 131 is stored is first chosen by the settlement system 100 publishing a file selection command to IC card 101 using logical channel A. It continues, and by publishing a command with the specific settlement system 100 to the service program 131 using logical channel A, processing based on the service program 131 is performed until PIN attestation is needed.

[0061]Here, before performing PIN attestation, the settlement system 100 publishes a file selection command to IC card 101, using logical channel B as Step S702, and chooses the

dedicated file in which the PIN control program 132 is stored.

[0062]Next, when the cardholder 102 inputs common PIN into the settlement system 100, the settlement system 100 transmits common PIN to IC card 101, and has individual PIN replied from IC card 101 as Step S703. In this processing, the settlement system 100 publishes an individual PIN acquisition command to the PIN control program 132 using logical channel B. Here, a flag with which individual PIN corresponding to common PIN and the service program 131 to application-identifier-AID and acquire expresses an object for on-line or an object for off-line shall be stored in an individual PIN acquisition command. If these data is acquired, according to procedure explained using drawing 4 by a 1st embodiment, the PIN control program 132 will extract individual PIN, and will reply it to the settlement system 100.

[0063]Next, the settlement system 100 confirms whether perform PIN attestation off-line or carry out on-line as Step S704.

[0064]If off-line PIN attestation is performed, the settlement system 100 will transmit acquired individual PIN to IC card 101 as Step S705. The settlement system 100 is publishing an PIN verification command to the service program 131, and makes individual PIN compare by IC card 101 inside in this processing.

[0065]On the other hand, if on-line attestation is performed, the settlement system 100 transmits acquired individual PIN to a center via a network as Step S706.

[0066]After off-line PIN attestation or on-line PIN attestation is completed according to a procedure explained above, as Step S707, the terminal 100 is specific to IC card 101, carries out command issue of the remaining settling processings to it, and is continued.

[0067]Next, a 3rd embodiment is described. Composition of an IC card and a settlement system concerning this embodiment and composition of information stored in an IC card are the same as composition explained by a 2nd embodiment. Furthermore, in this embodiment, an PIN control program stored in IC card 101 or two or more service programs are IC card 101 insides, and let them be what has possible transmitting and receiving a command of APDU form mutually. Such processing is realizable by using a "delegation function" which is one of the functions which MULTOS known as an operating system for IC cards has, for example.

[0068]This delegation function is explained using drawing 8. In drawing 8, the program A650 and the program B651 are stored in IC card 101. First, when the settlement system 100 publishes the command A of APDU form to the program A650, the program A650 publishes the command B of APDU form to the program B651, and makes the program B651 execute arbitrary processings by proxy. Next, the program B651 is returned to the program A650 by making a result of vicarious execution processing into the response B. And the program A650 returns the response A to the settlement system 100 based on a result of the response B.

[0069]As explained above, if a program with IC card 101 inside receives a command from the IC card 101 exterior, The function made to execute by proxy by transmitting a command to

other programs which are in IC card 101 inside in a part of processing performed based on the received command is called a delegation function.

[0070]In this embodiment, although the delegation function mentioned above is used, it does not matter even if it is the composition using other operating systems which have a function equivalent to a delegation function as an operating system of an IC card even if it does not use MULTOS.

[0071]Next, the process flow of the settlement system 100 concerning this embodiment is explained. Drawing 9 is a flow chart in case the cardholder 102 performs settling processing with the settlement system 100 using IC card 101. In this example, the command which the settlement system 100 transmits to IC card 101 shall use APDU form. The IC card stores the service program 131 and the PIN control program 132, and the settlement system 100, It shall communicate simultaneously, using logical channel B as a logical channel number of the command published to the PIN control program 132 using logical channel A as a logical channel number of the command published to the service program 131.

[0072]First, if IC card 101 is inserted in the settlement system 100, initialization processing of an IC card will be performed as Step S800. In this processing, the settlement system 100 transmits a reset request to IC card 101, and receiving a reset response from IC card 101 after that is performed.

[0073]Next, the settlement system 100 chooses the service program 131 stored in IC card 101 by the cardholder's 102 selection, etc. as Step S801. In this processing, a dedicated file in which the service program 131 is stored is first chosen by the settlement system 100 publishing a file selection command to IC card 101 using logical channel A. It continues, and processing based on the service program 131 is performed until PIN attestation is needed, because the settlement system 100 publishes a specific command to the service program 131 using logical channel A.

[0074]Here, before performing PIN attestation, the settlement system 100 publishes a file selection command to IC card 101, using logical channel B as Step S802, and chooses a dedicated file in which the PIN control program 132 is stored.

[0075]Next, when the cardholder 102 inputs common PIN into the settlement system 100, the settlement system 100 transmits common PIN to IC card 101, and makes PIN verification perform by IC card 101 inside as Step S803. In this processing, the settlement system 100 publishes an PIN verification command to the PIN control program 132 first using logical channel B. Here, common PIN and the application identifier AID corresponding to the service program 131 shall be stored in an PIN verification command. Next, the PIN control program 132 will extract individual PIN according to procedure explained using drawing 4 by a 1st embodiment, if these data is acquired. Next, the PIN control program 132 publishes an PIN verification command which stored extracted individual PIN to the service program 131, makes

individual PIN compare with the service program 131, and acquires a matching result. And the PIN control program 132 replies a matching result to the settlement system 100. Here, processing of Step S803 is realizable by using a delegation function mentioned above.

[0076]After PIN attestation is completed according to the procedure explained above, as Step S804, the terminal 100 is specific to IC card 101, carries out command issue of the remaining settling processings to it, and is continued.

[0077]Next, a 4th embodiment is described. First, the composition of the IC card and settlement system concerning this embodiment is shown in drawing 10. Although the composition shown in drawing 10 is the same as the composition shown in drawing 1 by explanation of a 1st embodiment, the point that the PIN input means 113 replaced the fingerprint reading means 190 differs from the point that the cardholder 102 does not need to memorize common PIN105.

[0078]Here, the fingerprint reading means 190 identifies the cardholder's 102 fingerprint, and has the function to extract fingerprint information. therefore -- it is that the cardholder 102 makes his fingerprint identify by the fingerprint reading means 190 in this embodiment instead of inputting PIN into the settlement system 100 -- the person himself/herself -- it attests.

[0079]Next, the composition of the information stored in the IC card concerning this embodiment is shown in drawing 11. Although the composition shown in drawing 11 is the same as the composition shown in drawing 2 by explanation of a 1st embodiment, It differs in that AID, the data 144A, 144B, and 144C which comprises individual PIN, and the fingerprint information 191 are stored instead of storing the PIN management data 142A, 142B, and 142C in the PIN management dedicated file 122. Here, AID which constitutes the data 144A corresponds to the dedicated file 121A, and individual PIN is used for the off-line PIN attestation performed by the service program 131A stored in the dedicated file 121A. Similarly AID which constitutes the data 144B corresponds to the dedicated file 121B, and individual PIN is used for the off-line PIN attestation performed by the service program 131B. AID which constitutes the data 144C corresponds to the dedicated file 121C, and individual PIN is used for the on-line PIN attestation performed by the service program 131C. The fingerprint information 191 is information corresponding to the cardholder's 102 fingerprint. Unless collation of the fingerprint information 191 is successful, it has come to be unable to perform reading the data 144A, 144B, and 144C to the exterior here.

[0080]Next, a process flow of the settlement system 100 concerning this embodiment is explained. Drawing 12 is a flow chart in case the cardholder 102 performs settling processing with the settlement system 100 using IC card 101. Although a flow chart shown in drawing 12 is the same to a flow shown in drawing 7 by explanation of a 2nd embodiment, and Step S702, it differs in that the cardholder 102 is making the settlement system 100 identify a fingerprint instead of inputting common PIN into the settlement system 100.

[0081] That is, a fingerprint which the settlement system 100 identified is changed into fingerprint information by a fingerprint reading means, and the settlement system 100 transmits fingerprint information to IC card 101, and has specific individual PIN replied from IC card 101 in Step S1000. In this processing, the settlement system 100 publishes an individual PIN acquisition command to the PIN control program 132. An application identifier corresponding to fingerprint information and the service program 131 is stored in an individual PIN command here, and the PIN control program 132, When an individual PIN command was received, fingerprint information is compared and collation is successful, individual PIN corresponding to a specified application identifier is returned to the settlement system 100. The settlement system 100 is using this individual PIN, and it becomes possible to perform the same PIN attestation as a 2nd embodiment.

[0082] As explained above, when the cardholder 102 receives one which can be performed of services using IC card 101, in this embodiment, it becomes possible to make the settlement system 100 only identify a fingerprint, and to perform PIN attestation which needs to be performed for every service. The cardholder 102 inputs common PIN here instead of making the settlement system 100 identify a fingerprint, When common PIN is recorded and collation of common PIN is successful within IC card 101 instead of recording fingerprint information on IC card 101, even if it is the composition which can read individual PIN from an IC card, it is a scope of this invention.

[0083]

[Effect of the Invention] As explained above, when an IC card owner receives each service using the IC card corresponding to two or more services according to this invention, It becomes possible to improve an IC card owner's convenience by having composition which can be performed only by making a fingerprint identify as one common PIN is kept in mind for the PIN attestation which needs to be performed for every service.

TECHNICAL FIELD

[Field of the Invention]an IC card is used for this invention -- the person himself/herself -- it is related with the IC card terminal equipment and the person-himself/herself authentication method which attest.

PRIOR ART

[Description of the Prior Art]In recent years, an IC card is spreading widely instead of a magnetic card. This is because there is the feature provided with the arithmetic unit (microprocessor) for performing cipher processing with a large storage capacity, etc. which is not in a magnetic card that an inside can be observed easily and nothing is (it has the Tampa-proof nature) in an IC card. By applying an IC card with such a feature to a settlement system, an identification system, etc., security can be raised compared with a magnetic card, or the new service which was not able to be realized in a magnetic card can be provided. For example, there are electronic money and a credit card as service which a settlement system provides, and an employee ID card, a driver's license, etc. are raised as service which an identification system provides.

[0003]The IC card is classified into the contact type and the noncontact type according to the communication method.

Each specification is already standardized.

For example, a contact smart card is ISO (International Organization for Standardization: International Organization for Standardization), and is standardized as ISO/IEC7816. The IC card based on ISO/IEC7816 calculates inside according to the command which transmits from a terminal, is performing returning a result as a response one by one, and carries out processing for realizing service.

[0004]Here, the command and response which are transmitted and received between IC card terminals are specified in the form of APDU (Application Protocol Data Unit) ISO/IEC7816. The IC card based on ISO/IEC7816 is stored in the file in which a program and data had a layered structure as shown in drawing 13.

[0005]In drawing 13, the main file (MF) 900 is a file of a top layer, and exists only one in an IC card, and two or more dedicated file (DF)901A, and 901B and 901C exist in the bottom of it. Data (it is called service information below) required for the program (it is called the service program below) and service execution for performing specific service is stored in a dedicated file. Since two or more existence is possible for a dedicated file in an IC card, two or more services can be used by the IC card of one sheet by storing two or more service programs and service information in a different dedicated file.

[0006]In order to execute a specific service program, a terminal chooses first the dedicated file in which the specific service program is stored as a file of KARENTO using the "file selection command" specified as a command of APDU form. Thereby, the command which an IC card receives from a terminal after it comes to be processed according to the selected service program. Here, each dedicated file is identifiable from the outside by ID called an application identifier (it omits the following AID). For example, the "file selection command" can choose a

specific dedicated file by specifying AID.

[0007]now, the case where service is received using an IC card -- a cardholder -- the attestation which it may be urged to attest that the person himself/herself is using that card, for this reason it performs -- the person himself/herself -- it is called attestation. The PIN attestation as which a cardholder inputs the password called PIN into a terminal as a method for realizing person-himself/herself attestation is common. PIN attestation includes "off-line PIN attestation" compared with PIN which has memorized PIN which the cardholder inputted in an IC card, and "on-line PIN attestation" compared with PIN in which the center holds PIN which the cardholder inputted via a network. the persons themselves himself/herself, such as PIN attestation, -- attesting is important in order to prevent the illegal use of an IC card.

EFFECT OF THE INVENTION

[Effect of the Invention]As explained above, when an IC card owner receives each service using the IC card corresponding to two or more services according to this invention, It becomes possible to improve an IC card owner's convenience by having composition which can be performed only by making a fingerprint identify as one common PIN is kept in mind for the PIN attestation which needs to be performed for every service.

EFFECT OF THE INVENTION

[Effect of the Invention]As explained above, when an IC card owner receives each service using the IC card corresponding to two or more services according to this invention, It becomes possible to improve an IC card owner's convenience by having composition which can be performed only by making a fingerprint identify as one common PIN is kept in mind for the PIN attestation which needs to be performed for every service.

TECHNICAL PROBLEM

[Problem to be solved by the invention]As explained above, can use various services by an IC card of one sheet by using an IC card, but. On the other hand, in order to use each service, when performing PIN attestation, a cardholder keeps different PIN for every service in mind, and may have to use PIN properly for every service to be used. This becomes a factor which spoils a card user's convenience greatly.

[0009]Then, when this invention receives each service using an IC card corresponding to two or more services in an IC card owner, an IC card terminal which can improve an IC card owner's convenience by carrying out PIN attestation which needs to be performed for every service to composition which can be performed only by keeping one common PIN in mind, and the person himself/herself -- it aims at providing an authentication method.

MEANS

[Means for solving problem]In this invention, the service program to process the service which needs a cardholder's justification check To achieve the above objects, one or more pieces, The individual password used in order to perform said cardholder's justification check One or more pieces, The password inputting means as which said cardholder can input the 1st password in the IC card terminal using the IC card one or more encryption passwords which enciphered said individual password were remembered to be, The card write means which communicates with said IC card, and the information accumulation means which accumulates the information acquired from said IC card, Said encryption password is read from said IC card by said card write means, Said encryption password which was accumulated in said information accumulation means and accumulated in said information accumulation means is read, Decrypt by said 1st password, generate the 2nd password, and said 2nd password is transmitted to said IC card by said card write means, When said 2nd password is in agreement with said individual password inside said IC card, it has an arithmetic processing means which carries out normal execution of said service.

[0011]In this invention, a service program to process service which needs a cardholder's justification check One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, An IC card one or more encryption passwords which enciphered said individual password were remembered to be, the person himself/herself in a system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- an authentication method with a processing step to which said IC card terminal reads said encryption password from said IC card. A processing step which accumulates said encryption password which said IC card terminal read from said IC card, A processing step as which said card holder inputs the 1st password into said IC card terminal, A processing step which decrypts said encryption password which said IC card terminal is accumulating by said 1st password, and generates the 2nd password, When said IC card terminal transmits said 2nd password to said IC card and said 2nd password is in agreement with said individual password inside said IC card, a processing step which carries out normal execution of said service is included.

[0012]Namely, in order to solve an aforementioned problem, this invention, A service program to process service which needs a cardholder's justification check One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, A password inputting means as which said cardholder can input the 1st password in an IC card terminal using an IC card one or more encryption passwords which enciphered said individual password were remembered to be, A card write means which communicates with said IC card, and said encryption password are read from said IC card by said card write

means, Decrypt by said 1st password and it has an arithmetic processing means which transmits the 2nd password that generated and generated the 2nd password to said IC card by said card write means, When said 2nd password was in agreement with said individual password inside said IC card, it was made to carry out normal execution of said service.

[0013]This invention establishes an information accumulation means which accumulates information acquired from said IC card in the above-mentioned IC card terminal, and reads said encryption password from said IC card by said card write means, Said encryption password which was accumulated in this information accumulation means and accumulated in this information accumulation means is read, and it was made to decode by the 1st password.

[0014]In the above-mentioned IC card terminal, this invention said encryption password, Encipher using said 1st password and what combined said individual password and fixed value data which consists of a specific value said arithmetic processing means, When said fixed value data corrected to data which decrypted said encryption password using said 1st password and ** was contained in it, we decided to judge that said said 2nd password produced by decrypting is equal to said individual password.

[0015]In order to solve an aforementioned problem, a service program which processes service which needs a cardholder's justification check this invention One or more pieces, An IC card one or more encryption passwords which enciphered an individual password used in order to perform said cardholder's justification check were remembered to be is used, A password inputting means as which said cardholder can input the 1st password in an IC card terminal which communicates with a center apparatus which is keeping said individual password, A card write means which communicates with said IC card, and a means of communication which communicates with said center apparatus via a network, Said encryption password read from said IC card by said card write means is decrypted by said 1st password, When the 2nd password was generated, it had an arithmetic processing means which transmits said 2nd password to said center apparatus by said means of communication and said 2nd password was in agreement with said individual password with said center apparatus, we decided to carry out normal execution of said service.

[0016]This invention establishes the information accumulation means which accumulates the information acquired from said IC card in the above-mentioned IC card terminal, and reads said encryption password from said IC card by said card write means, Said encryption password which was accumulated in this information accumulation means and accumulated in this information accumulation means is read, and it was made to decode by the 1st password.

[0017]In the above-mentioned IC card terminal, this invention said encryption password, Encipher using said 1st password and what combined said individual password and the fixed value data which consists of a specific value said arithmetic processing means, When said fixed value data corrected to the data which decrypted said encryption password using said 1st

password and ** was contained in it, we decided to judge that said said 2nd password produced by decrypting is equal to said individual password.

[0018]In order to solve an aforementioned problem, the service program which processes the service which needs a cardholder's justification check this invention One or more pieces, The individual password used in order to perform said cardholder's justification check One or more pieces, The IC card one or more encryption passwords which enciphered said individual password were remembered to be, the person himself/herself in the system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- an authentication method with the processing step to which said IC card terminal reads said encryption password from said IC card. The processing step which accumulates said encryption password which said IC card terminal read from said IC card, The processing step as which said card holder inputs the 1st password into said IC card terminal, The processing step which decrypts said encryption password which said IC card terminal is accumulating by said 1st password, and generates the 2nd password, When said IC card terminal transmitted said 2nd password to said IC card and said 2nd password was in agreement with said individual password inside said IC card, it was made for the processing step which carries out normal execution of said service to be included.

[0019]In order to solve an aforementioned problem, the service program which processes the service which needs a cardholder's justification check this invention One or more pieces, The IC card one or more encryption passwords which enciphered the individual password used in order to perform said cardholder's justification check were remembered to be, The IC card terminal which provides said service for said cardholder using said IC card, the person himself/herself in the system which consists of a center apparatus which is connected with said IC card terminal via the network, and is keeping said individual password -- an authentication method, The processing step to which said IC card terminal reads said encryption password from said IC card, The processing step which accumulates said encryption password which said IC card terminal read from said IC card, The processing step as which said card holder inputs the 1st password into said IC card terminal, The processing step which decrypts said encryption password which said IC card terminal is accumulating by said 1st password, and generates the 2nd password, When said IC card terminal transmits said 2nd password to said center apparatus and said 2nd password is in agreement with said individual password with said center apparatus, It was made for the processing step which carries out normal execution of said service to be included.

[0020]In order to solve an aforementioned problem, a service program which processes service which needs a cardholder's justification check this invention One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, An IC card a password control program in which an encryption password which

enciphered said individual password manages one or more pieces and said encryption password was remembered to be, the person himself/herself in a system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- an authentication method with a processing step as which said cardholder inputs the 1st password into said IC card terminal. A processing step at which said IC card terminal transmits said 1st password to said IC card, Said password control program executed within said IC card decrypts said encryption password by said 1st password, and generates the 2nd password, It was made for a processing step which transmits to said IC card terminal, and a processing step which carries out normal execution of said service when said IC card terminal transmits said 2nd password to said IC card and said 2nd password is in agreement with said individual password inside said IC card to be included.

[0021]In order to solve an aforementioned problem, a service program which processes service which needs a cardholder's justification check this invention One or more pieces, An individual password used in order to perform said cardholder's justification check One or more pieces, An IC card a password control program in which an encryption password which enciphered said individual password manages one or more pieces and said encryption password was remembered to be, the person himself/herself in a system which consists of an IC card terminal which provides said service for said cardholder using said IC card -- an authentication method with a processing step as which said card holder inputs the 1st password into said IC card terminal. A processing step at which said IC card terminal transmits said 1st password to said IC card, A processing step which said password control program executed within said IC card decrypts said encryption password by said 1st password, and generates the 2nd password, When said password program transmitted the 2nd password to said service program and said 2nd password was in agreement with said individual password, it was made for a processing step which carries out normal execution of said service to be included.

[0022]This invention is provided with the following in order to solve an aforementioned problem.

The service program which processes the service which needs a cardholder's justification check is one or more pieces.

The individual password used in order to perform said cardholder's justification check is one or more pieces.

The password inputting means as which said cardholder can input the 2nd password in the IC card terminal which provides for said cardholder the **** aforementioned service for IC cards the 1st password that protects outputting said individual password outside was remembered to be.

Transmit to said IC card by said IC card write means, and the card write means which

communicates with said IC card, and said 2nd password inside said IC card, When said 2nd password is in agreement with said 1st password, acquire said individual password by said IC card write means, and said individual password is transmitted to said IC card by said card write means, The arithmetic processing means which carries out normal execution of said service when collation of said individual password inside said IC card is successful.

[0023]This invention is provided with the following in order to solve an aforementioned problem.

The service program which processes the service which needs a cardholder's justification check is one or more pieces.

The individual password used in order to perform said cardholder's justification check is one or more pieces.

The 1st biological information that protects outputting said individual password outside.

The biological information reading means in which the IC card terminal which provides said service for said cardholder using the IC card the control program which manages biological information was remembered to be can read the 2nd biological information in said cardholder, Transmit the card write means which communicates with said IC card, and said 2nd biological information to said IC card by said IC card write means, and inside said IC card, When said 2nd biological information is in agreement with said 1st biological information, acquire said individual password by said IC card write means, and said individual password is transmitted to said IC card by said card write means, The arithmetic processing means which carries out normal execution of said service when collation of said individual password inside said IC card is successful.

[0024]In the above-mentioned IC card terminal, a fingerprint was used for this invention as said 1st biological information and said 2nd biological information.

[0025]

[Mode for carrying out the invention]Hereafter, an embodiment of this invention is described.

Although following embodiments explain a case where an IC card of a contact type is used, it is not an item required for this invention that it is a contact type, for example, this invention is here, applicable even if it is a noncontact IC card. In following embodiments, although a command transmitted and received between a terminal and an IC card assumes a command of APDU form, If it is a command set which it is not an item required for this invention to use a command of APDU form, and can realize a function equivalent to APDU form, this invention is applicable no matter what thing it may use. not an item in which it is required for this invention to be such a terminal although a terminal with a function to perform settlement of accounts for electronic money or a credit card as a terminal is assumed in following embodiments but the

person himself/herself -- this invention is applicable if it is a terminal which attests.

[0026]First, a 1st embodiment is described. drawing 1 -- the person himself/herself -- composition of an IC card and a terminal concerning this embodiment which attests is shown. in drawing 1 -- the person himself/herself -- attestation is performed between the settlement system 100, IC card 101, the cardholder 102, the salesclerk 103, and the network 104. Composition shown in drawing 1 assumes that the cardholder 102 performs settlement of accounts by electronic money or a credit card using IC card 101. Therefore, the settlement system 100 is a terminal provided with a clearing function by an IC card, for example, assumes ATM of a credit terminal or a financial institution. IC card 101 has composition that service of plurality, such as electronic money and a credit card, can be provided. the cardholder 102 -- the person himself/herself -- suppose that common PIN105 which can be used in common with two or more services which are PIN used for attestation and IC card 101 provides is memorized.

[0027]Next, an internal configuration of the settlement system 100 is explained. The settlement system 100 has the card write means 110, the arithmetic processing means 111, the display device 112, the PIN input means 113, the information accumulation means 114, the control means 115, and the means of communication 116.

[0028]The card write means 110 has the function to transmit a command to IC card 101 (writing), or to receive a response from an IC card (reading), in order to communicate with IC card 101.

[0029]The arithmetic processing means 111 comprises a microprocessor and a program storing memory, for example, controls the settlement system 100 whole based on a program stored in a program storing memory, and has a function which carries out settling processing.

[0030]The displaying means 112 displays a variety of information of a settlement amount etc. as opposed to the cardholder 102.

[0031]the PIN input means 113 -- the cardholder 102 -- the person himself/herself -- it has a function in which PIN for attestation can be inputted, for example using a ten key etc.

[0032]The information accumulation means 114 has a function which accumulates temporarily or permanently information acquired from IC card 101 or the network 104, or information which the cardholder 102 and the salesclerk 103 inputted, for example, comprises a hard disk, semiconductor memory, etc.

[0033]The control means 115 provides Interface Division for the salesclerk 103 to operate the settlement system 100, for example, comprises a keyboard, a bar code reader, a display, etc.

[0034]The means of communication 116 is used in order to have a function which communicates with a center via the network 104, for example, to perform on-line PIN attestation. Here, in the case of unmanned terminals, such as financial institution ATM, the control means 115 may not be, and, in the salesclerk 103, the settlement system 100 does not

need to exist. When settling processing by the settlement system 100 is completed off-line, there may not be the means of communication 116.

[0035]Next, an internal configuration of IC card 101 is explained. IC card 101 has the means of communication 117, the information accumulation means 118, and the arithmetic processing means 119.

[0036]The means of communication 117 communicates with the card write means 110 of the settlement system 100, and has the function to receive a command from the settlement system 100, or to reply a response to the settlement system 100.

[0037]A program and data in which the information accumulation means 118 performs service which an IC card provides, Or it has the function to store information etc. which were acquired from the settlement system 100 temporarily or permanently, for example, comprises semiconductor memory, such as ROM (Read Only Memory), RAM (Random Access Memory), and a flash memory.

[0038]The arithmetic processing means 119 is using a microprocessor, manages control of the whole IC card and has the function to execute a program stored in the information accumulation means 118.

[0039]Next, composition of information stored in IC card 101 concerning this embodiment is shown in drawing 2. Drawing 2 is the file organization of information accumulation means 118 inside which constitutes IC card 101, and comprises the main file (MF) 120, dedicated file (DF) 121A, 121B and 121C, and the PIN management dedicated file 122. These files have a layered structure and have composition that the main file 120 is located in the top and the dedicated files 121A, 121B, and 121C and the PIN management dedicated file 122 are located in the lower layer. Different AID is assigned to each dedicated file and it is identifiable from the outside.

[0040]Next, an internal configuration of the dedicated files 121A, 121B, and 121C is explained. in the service program 131A which performs specific account settlement services in the dedicated file 121A, and these account settlement services -- the person himself/herself -- individual PIN141A which is data required in order to perform attestation by off-line PIN attestation is stored. The service program 131B and individual PIN141B are similarly stored in the dedicated file 121B. account settlement services which the service program 131C is stored in the dedicated file 121C, and are performed by the service program 131C -- the person himself/herself -- on-line PIN attestation shall be performed as attestation Therefore, PIN data is not stored in the dedicated file 121C.

[0041]Next, the PIN management dedicated file 122 is explained. The PIN management dedicated file 122 is a dedicated file for PIN management. The PIN control program 132 which manages individual PIN individually used for the PIN management dedicated file 122 with the service programs 131A, 131B, and 131C, The PIN management data 142A, 142B, and 142C

which is data which the PIN control program 132 manages is stored. Data which needs the PIN management data 142A for off-line PIN attestation performed by the service program 131A here is contained. Similarly, data which needs the PIN management data 142B for off-line PIN attestation performed by the service program 131B is contained. Data which needs the PIN management data 142C for on-line PIN attestation performed by the service program 131C is contained.

[0042]Although three service programs are contained in the information accumulation means 118 and the PIN control program has the composition of having managed three PIN management data, in this explanation, this invention is applicable also to the IC card in which arbitrary numbers of service programs are contained. For example, when IC card 101 contains four service programs, the PIN control program should just manage four PIN management data. This invention is applicable even if it is the composition of performing off-line PIN attestation even if the service program in IC card 101 is the composition of performing on-line PIN attestation.

[0043]Next, the composition and the directions for PIN management data which the PIN control program 132 concerning this embodiment has managed are explained. First, the composition and the generation procedure of PIN management data are shown in drawing 3. In drawing 3, the PIN management data 142 has AID202, the control flag 203, and the composition that encryption individual PIN204 is contained. AID202 is an application identifier of the dedicated file in which the service program with which the PIN management data 142 corresponds is stored. The control flag 203 shows the PIN authentic method (on-line or off-line) with which the PIN management data 142 corresponds. For example, 1 bit shall be assigned to the control flag 203 and, in the case of individual PIN for on-line in the case of "0", and "1", individual PIN for off-line shall be held at the PIN management data 142. Encryption individual PIN204 enciphers individual PIN and the contents of original individual PIN cannot be guessed only from encryption individual PIN204.

[0044]As a generation procedure of the PIN management data 142, right AID202 is first set up as Step S200. Next, the right control flag 203 is set up as Step S201. Next, encryption processing is performed by using as an encryption key common PIN105 to which the cardholder set the data which combined individual PIN141 and the fixed pattern 201 as Step S202, and the cryptogram outputted is set to encryption individual PIN204. Here, the fixed pattern 201 is a certain specific bit string, and is defined as a fixed value. It is possible to use DES which is a cryptographic algorithm based on a block cipher system, for example as encryption processing performed at Step S202. Or other encryption algorithms may be used.

[0045]The above generation procedure is performed, when registering the PIN management data 142 newly and changing common PIN105, and when changing individual PIN141. What is necessary is just to replace with old PIN management data the PIN management data

generated by new common PIN, when changing common PIN. What is necessary is similarly, just to replace with old PIN management data the PIN management data generated from new individual PIN, when changing individual PIN.

[0046]Next, procedure which extracts individual PIN from PIN management data is shown in drawing 4. This procedure is performed by using the arithmetic processing means 111 which constitutes the settlement system 100 shown in drawing 1. In drawing 4, the PIN management data 142 has AID202, the control flag 203, and composition that encryption individual PIN204 is contained, as mentioned above.

[0047]First, it is investigated whether it is in agreement with an application identifier of a dedicated file in which a service program which checks AID202 and uses individual PIN as Step S300 is stored. If AID is not in agreement, the end of this processing of unjust is carried out. If AID is in agreement, next, as Step S301, the control flag 203 will be checked and it will be investigated whether the control flag 203, a shown PIN authentic method (off-line or on-line), and an PIN authentic method which a service program which uses individual PIN holds are in agreement. If an PIN authentic method is not in agreement, the end of the processing of unjust is carried out. When an PIN authentic method is in agreement, next, as Step S302, by using common PIN105 as an encryption key, decoding processing is performed and a plaintext outputted is divided into individual PIN141 and the fixed pattern 201. Here, as common PIN105, the cardholder 102 uses what was inputted into the terminal 100.

[0048]Next, it is verified whether the acquired fixed pattern 201 is a right value as Step S303. Here, the terminal 100 presupposes that a right value of a fixed pattern is known beforehand. If the fixed pattern 201 is not a right value, the end of this processing of unjust will be carried out. If the fixed pattern 201 is a right value, it will consider that individual PIN141 has been acquired correctly and normal termination of this processing will be carried out.

[0049]Next, a process flow of the settlement system 100 concerning this embodiment is explained. Drawing 5 is a flow chart in case the cardholder 102 performs settling processing with the settlement system 100 using IC card 101. Here, this settling processing shall be performed using the arithmetic processing means 111 which constitutes the settlement system 100 shown by drawing 1. In this example, although an IC card stores the service program 131 and the PIN control program 132, the settlement system 100 shall not communicate simultaneously with two or more programs stored in IC card 101. A command which the settlement system 100 transmits to IC card 101 is explained as what uses APDU form.

[0050]First, if IC card 101 is inserted in the settlement system 100, initialization processing of an IC card will be performed as Step S500. In this processing, the settlement system 100 transmits a reset request to IC card 101, and receiving a reset response from IC card 101 after that is performed. Next, the settlement system 100 reads all the PIN management data stored in IC card 101 as Step S501. In this processing, the settlement system 100 chooses first the

PIN management dedicated file in which the PIN control program 132 is stored by publishing a file selection command to IC card 101. The PIN management data 142 is altogether read because continue and the settlement system 100 publishes a data readout command to the PIN control program 132. The read PIN management data is stored in the information accumulation means 114 shown in drawing 1.

[0051]Next, the terminal 100 chooses the service program 131 stored in IC card 101 by the cardholder's 102 selection, etc. as Step S502. In this processing, the settlement system 100 chooses first the dedicated file in which the service program 131 is stored by publishing a file selection command to IC card 101. It continues, and by publishing a command with the specific settlement system 100 to the service program 131, processing based on the service program 131 is performed until PIN attestation is needed.

[0052]Next, the cardholder's 102 input of common PIN105 will decode individual PIN as Step S503 from the PIN management data previously read from the IC card using common PIN inputted into the terminal 100. In this processing, it performs until it succeeds the processing which extracts individual PIN explained using drawing 4 to all the PIN management data read from the IC card. Here, if the extracting processing of individual PIN ends in failure, the operation method of interrupting settling processing will be considered first. Or if the extracting processing of individual PIN goes wrong, the operation method of continuing settling processing after considering that common PIN inputted into the terminal 100 is individual PIN will also be considered. About the case of the latter, the cardholder 102 becomes an operation method in the case of inputting either common PIN or individual PIN as Step S503.

[0053]Next, it confirms whether perform PIN attestation off-line or carry out on-line as Step S504. Supposing it performs off-line PIN attestation, the settlement system 100 will transmit extracted individual PIN to IC card 101 as Step S505. The settlement system 100 is publishing an PIN verification command to the service program 131, transmits individual PIN to IC card 101, and makes individual PIN compare inside in this processing. If one side is also carried out and on-line attestation is performed, the settlement system 100 transmits extracted individual PIN to a center via a network as Step S506. After off-line PIN attestation or on-line PIN attestation is completed according to the procedure explained above, as Step S507, the terminal 100 is specific to IC card 101, carries out command issue of the remaining settling processings to it, and is continued.

[0054]Next, a 2nd embodiment is described. The composition of the IC card and settlement system concerning this embodiment is the same as the composition shown by explanation using drawing 1 by a 1st embodiment. The composition of the information stored in the IC card concerning this embodiment is the same as the composition explained using drawing 2 by a 1st embodiment. The procedure which extracts individual PIN from PIN management data is the same as the procedure explained using drawing 4 by a 1st embodiment. However,

according to this embodiment, let the terminal 100 be what has possible communicating with the PIN control program stored in IC card 101, and two or more service programs simultaneously. In this embodiment, the PIN control program 132 stored in IC card 101 shall perform processing which extracts individual PIN from PIN management data.

[0055]Hereafter, the realization method of this embodiment is shown. First, drawing 6 is a block diagram of the command of APDU form. In drawing 6, the command of APUD form comprises the class 610, the command 611, the parameter 1 (612), the parameter 2 (613), Lc614, the data 615, and Le616. The class 610 is an identifier of the service program which communicates using a command. The command 611 shows the instruction code of a command. The parameter 1 (612) and the parameter 2 (613) store the value of the parameter depending on the command 611. Lc614 expresses the length of the data 615 which is the next field. The data 615 is the field which stores the data transmitted to an IC card. Le616 expresses the length of the response returned from an IC card.

[0056]In drawing 6, the class 610 comprises the command type 620, the security message type 621, and the logical channel number 622. The command type 620 is the field for classifying the command 611. A security message type is the field showing whether encryption processing for preventing tapping and an alteration of the data 615 is performed. The logical channel number 622 is used in order to distinguish a command published to a program stored in an IC card using a logical address. That is, it becomes possible by changing a value of the logical channel number 622 to communicate with two or more programs in an IC card simultaneously.

[0057]In the above explanation, although explained taking the case of a command of APDU form, if it has a function equivalent to a function using a logical channel, even if it is a command of other forms, it is applicable to this invention.

[0058]Next, a process flow of the settlement system 100 concerning this embodiment is explained. Drawing 7 is a flow chart in case the cardholder 102 performs settling processing with the settlement system 100 using IC card 101. This example explains a command which the settlement system 100 transmits to IC card 101 as what uses APDU form. An IC card stores the service program 131 and the PIN control program 132, and the settlement system 100, It shall communicate simultaneously, using logical channel B as a logical channel number of a command published to the PIN control program 132 using logical channel A as a logical channel number of a command published to the service program 131.

[0059]First, if IC card 101 is inserted in the settlement system 100, initialization processing of an IC card will be performed as Step S700. In this processing, the settlement system 100 transmits a reset request to IC card 101, and receiving a reset response from IC card 101 after that is performed.

[0060]Next, the settlement system 100 chooses the service program 131 stored in IC card 101

by the cardholder's 102 selection, etc. as Step S701. In this processing, a dedicated file in which the service program 131 is stored is first chosen by the settlement system 100 publishing a file selection command to IC card 101 using logical channel A. It continues, and by publishing a command with the specific settlement system 100 to the service program 131 using logical channel A, processing based on the service program 131 is performed until PIN attestation is needed.

[0061]Here, before performing PIN attestation, the settlement system 100 publishes a file selection command to IC card 101, using logical channel B as Step S702, and chooses a dedicated file in which the PIN control program 132 is stored.

[0062]Next, when the cardholder 102 inputs common PIN into the settlement system 100, the settlement system 100 transmits common PIN to IC card 101, and has individual PIN replied from IC card 101 as Step S703. In this processing, the settlement system 100 publishes an individual PIN acquisition command to the PIN control program 132 using logical channel B. Here, a flag with which individual PIN corresponding to common PIN and the service program 131 to application-identifier-AID and acquire expresses an object for on-line or an object for off-line shall be stored in an individual PIN acquisition command. If these data is acquired, according to procedure explained using drawing 4 by a 1st embodiment, the PIN control program 132 will extract individual PIN, and will reply it to the settlement system 100.

[0063]Next, the settlement system 100 confirms whether perform PIN attestation off-line or carry out on-line as Step S704.

[0064]If off-line PIN attestation is performed, the settlement system 100 will transmit acquired individual PIN to IC card 101 as Step S705. The settlement system 100 is publishing a PIN verification command to the service program 131, and makes individual PIN compare by IC card 101 inside in this processing.

[0065]On the other hand, if on-line attestation is performed, the settlement system 100 transmits acquired individual PIN to a center via a network as Step S706.

[0066]After off-line PIN attestation or on-line PIN attestation is completed according to the procedure explained above, as Step S707, the terminal 100 is specific to IC card 101, carries out command issue of the remaining settling processings to it, and is continued.

[0067]Next, a 3rd embodiment is described. The composition of the IC card and settlement system concerning this embodiment and the composition of the information stored in an IC card are the same as the composition explained by a 2nd embodiment. Furthermore, in this embodiment, the PIN control program stored in IC card 101 or two or more service programs are IC card 101 insides, and let them be what has possible transmitting and receiving the command of APDU form mutually. Such processing is realizable by using the "delegation function" which is one of the functions which MULTOS known as an operating system for IC cards has, for example.

[0068]This delegation function is explained using drawing 8. In drawing 8, the program A650 and the program B651 are stored in IC card 101. First, when the settlement system 100 publishes the command A of APDU form to the program A650, the program A650 publishes the command B of APDU form to the program B651, and makes the program B651 execute arbitrary processings by proxy. Next, the program B651 is returned to the program A650 by making the result of vicarious execution processing into the response B. And the program A650 returns the response A to the settlement system 100 based on the result of the response B.

[0069]As explained above, if a program with IC card 101 inside receives a command from the IC card 101 exterior, The function made to execute by proxy by transmitting a command to other programs which are in IC card 101 inside in a part of processing performed based on the received command is called a delegation function.

[0070]In this embodiment, although the delegation function mentioned above is used, it does not matter even if it is the composition using other operating systems which have a function equivalent to a delegation function as an operating system of an IC card even if it does not use MULTOS.

[0071]Next, the process flow of the settlement system 100 concerning this embodiment is explained. Drawing 9 is a flow chart in case the cardholder 102 performs settling processing with the settlement system 100 using IC card 101. In this example, the command which the settlement system 100 transmits to IC card 101 shall use APDU form. The IC card stores the service program 131 and the PIN control program 132, and the settlement system 100, It shall communicate simultaneously, using logical channel B as a logical channel number of the command published to the PIN control program 132 using logical channel A as a logical channel number of the command published to the service program 131.

[0072]First, if IC card 101 is inserted in the settlement system 100, initialization processing of an IC card will be performed as Step S800. In this processing, the settlement system 100 transmits a reset request to IC card 101, and receiving a reset response from IC card 101 after that is performed.

[0073]Next, the settlement system 100 chooses the service program 131 stored in IC card 101 by the cardholder's 102 selection, etc. as Step S801. In this processing, the dedicated file in which the service program 131 is stored is first chosen by the settlement system 100 publishing a file selection command to IC card 101 using logical channel A. It continues, and processing based on the service program 131 is performed until PIN attestation is needed, because the settlement system 100 publishes a specific command to the service program 131 using logical channel A.

[0074]Here, before performing PIN attestation, the settlement system 100 publishes a file selection command to IC card 101, using logical channel B as Step S802, and chooses the

dedicated file in which the PIN control program 132 is stored.

[0075]Next, when the cardholder 102 inputs common PIN into the settlement system 100, the settlement system 100 transmits common PIN to IC card 101, and makes PIN verification perform by IC card 101 inside as Step S803. In this processing, the settlement system 100 publishes an PIN verification command to the PIN control program 132 first using logical channel B. Here, common PIN and the application identifier AID corresponding to the service program 131 shall be stored in an PIN verification command. Next, the PIN control program 132 will extract individual PIN according to the procedure explained using drawing 4 by a 1st embodiment, if these data is acquired. Next, the PIN control program 132 publishes the PIN verification command which stored extracted individual PIN to the service program 131, makes individual PIN compare with the service program 131, and acquires a matching result. And the PIN control program 132 replies a matching result to the settlement system 100. Here, processing of Step S803 is realizable by using the delegation function mentioned above.

[0076]After PIN attestation is completed according to the procedure explained above, as Step S804, the terminal 100 is specific to IC card 101, carries out command issue of the remaining settling processings to it, and is continued.

[0077]Next, a 4th embodiment is described. First, the composition of the IC card and settlement system concerning this embodiment is shown in drawing 10. Although the composition shown in drawing 10 is the same as the composition shown in drawing 1 by explanation of a 1st embodiment, the point that the PIN input means 113 replaced the fingerprint reading means 190 differs from the point that the cardholder 102 does not need to memorize common PIN105.

[0078]Here, the fingerprint reading means 190 identifies the cardholder's 102 fingerprint, and has the function to extract fingerprint information. therefore -- it is that the cardholder 102 makes his fingerprint identify by the fingerprint reading means 190 in this embodiment instead of inputting PIN into the settlement system 100 -- the person himself/herself -- it attests.

[0079]Next, the composition of the information stored in the IC card concerning this embodiment is shown in drawing 11. Although the composition shown in drawing 11 is the same as the composition shown in drawing 2 by explanation of a 1st embodiment, It differs in that AID, the data 144A, 144B, and 144C which comprises individual PIN, and the fingerprint information 191 are stored instead of storing the PIN management data 142A, 142B, and 142C in the PIN management dedicated file 122. Here, AID which constitutes the data 144A corresponds to the dedicated file 121A, and individual PIN is used for the off-line PIN attestation performed by the service program 131A stored in the dedicated file 121A. Similarly AID which constitutes the data 144B corresponds to the dedicated file 121B, and individual PIN is used for the off-line PIN attestation performed by the service program 131B. AID which constitutes the data 144C corresponds to the dedicated file 121C, and individual PIN is used

for the on-line PIN attestation performed by the service program 131C. The fingerprint information 191 is information corresponding to the cardholder's 102 fingerprint. Unless collation of the fingerprint information 191 is successful, it has come to be unable to perform reading the data 144A, 144B, and 144C to the exterior here.

[0080]Next, a process flow of the settlement system 100 concerning this embodiment is explained. Drawing 12 is a flow chart in case the cardholder 102 performs settling processing with the settlement system 100 using IC card 101. Although a flow chart shown in drawing 12 is the same to a flow shown in drawing 7 by explanation of a 2nd embodiment, and Step S702, it differs in that the cardholder 102 is making the settlement system 100 identify a fingerprint instead of inputting common PIN into the settlement system 100.

[0081]That is, a fingerprint which the settlement system 100 identified is changed into fingerprint information by a fingerprint reading means, and the settlement system 100 transmits fingerprint information to IC card 101, and has specific individual PIN replied from IC card 101 in Step S1000. In this processing, the settlement system 100 publishes an individual PIN acquisition command to the PIN control program 132. An application identifier corresponding to fingerprint information and the service program 131 is stored in an individual PIN command here, and the PIN control program 132, When an individual PIN command was received, fingerprint information is compared and collation is successful, individual PIN corresponding to a specified application identifier is returned to the settlement system 100. The settlement system 100 is using this individual PIN, and it becomes possible to perform the same PIN attestation as a 2nd embodiment.

[0082]As explained above, when the cardholder 102 receives one which can be performed of services using IC card 101, in this embodiment, it becomes possible to make the settlement system 100 only identify a fingerprint, and to perform PIN attestation which needs to be performed for every service. The cardholder 102 inputs common PIN here instead of making the settlement system 100 identify a fingerprint, When common PIN is recorded and collation of common PIN is successful within IC card 101 instead of recording fingerprint information on IC card 101, even if it is the composition which can read individual PIN from an IC card, it is a scope of this invention.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The figure showing the composition of the IC card and terminal concerning a 1st embodiment of this invention.

[Drawing 2]The figure showing the composition of the information stored in the IC card concerning a 1st embodiment of this invention.

[Drawing 3]The figure showing the composition and the generation procedure of the PIN management data concerning a 1st embodiment of this invention.

[Drawing 4]The figure showing the decoding procedure of the PIN management data concerning a 1st embodiment of this invention.

[Drawing 5]The figure showing the process flow of the settlement system concerning a 1st embodiment of this invention.

[Drawing 6]The figure showing the composition of the command concerning a 2nd embodiment of this invention.

[Drawing 7]The figure showing the process flow of the settlement system concerning a 2nd embodiment of this invention.

[Drawing 8]The figure showing the process flow of the communication between programs concerning a 3rd embodiment of this invention.

[Drawing 9]The figure showing the process flow of the settlement system concerning a 3rd embodiment of this invention.

[Drawing 10]The figure showing the composition of the IC card and terminal concerning a 4th embodiment of this invention.

[Drawing 11]The figure showing the composition of the information stored in the IC card concerning a 4th embodiment of this invention.

[Drawing 12]The figure showing the process flow of the settlement system concerning a 4th embodiment of this invention.

[Drawing 13]The figure showing the file organization of an IC card.

[Explanations of letters or numerals]

100 Settlement system

101 IC card

102 Cardholder

103 Salesclerk

104 Network

105 Common PIN

110 Card write means

111 Arithmetic processing means

- 112 A displaying means
- 113 An PIN input means
- 114 An information accumulation means
- 115 A control means
- 116 A means of communication
- 117 A means of communication
- 118 An information accumulation means
- 119 An arithmetic processing means